Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Maestría

Marco de Referencia Unificado en Seguridad de la Información

Autor: Esp. Lucas Falivene

Director: Prof. Raúl Saroka

Julio 2019

Cohorte: 2017

[Página dejada en blanco intencionalmente]

LICENCIA

Queda hecho el depósito que establece la Ley 11.723.

1° Edición – Julio 2019 – Buenos Aires, Argentina.

Bajo los siguientes términos

Atribución: en cualquier explotación de la obra autorizada por la licencia será necesario reconocer la autoría (obligatoria en todos los casos).

No Comercial: la explotación de la obra queda limitada a usos no comerciales.

Sin obras derivadas: la autorización para explotar la obra no incluye la posibilidad de crear una obra derivada.

[Página dejada en blanco intencionalmente]

DECLARACION JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis de Maestría vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Esp. Lucas I. Falivene
DNI 37.376.682

[Página dejada en blanco intencionalmente]

0.1 Resumen ejecutivo

El presente Trabajo Final de Maestría (TFM, en adelante) se enfoca en abordar la tarea de completar el Marco de Referencia Unificado en Seguridad de la Información (MRU, en adelante), cuyos lineamientos principales y dos de sus Subsistemas de Seguridad han sido desarrollados durante el Trabajo Final de Especialización (TFE, en adelante). Si bien dicho TFE se ha centrado en la definición de las bases primordiales del MRU (los Subsistemas de Lineamientos de SI y de Gobierno de SI), el TFM le dará un cierre a dicho desafío y centrará su alcance en la extensión del MRU, hasta su estadio de madurez "C"[1]. A su vez, incorporará complementos destinados a facilitar el camino a recorrer durante la implementación del MRU por parte de las organizaciones.

El TFM abordará adicionalmente la construcción de un macroproceso genérico de implementación del MRU. Dicha construcción se basará en el desarrollo de una metodología genérica, simple y ágil basada en la lógica de los procesos de negocio que logrará facilitar la tarea de los profesionales de Seguridad de la Información (SI, en adelante) al embarcarse en la implementación de los requerimientos del MRU. Su principal objetivo consiste en acompañar a las organizaciones desde su primera implementación del MRU hasta alcanzar el estadio de madurez "C" (el nivel de seguridad tope para la gran mayoría de las organizaciones, debido a la extensa complejidad requerida por el Modelo de Madurez de SI del MRU para los niveles superiores[2]) o el estadio de madurez "A" (el máximo nivel de seguridad, el cual simboliza la mejora continua en SI).

Por otro lado, a partir de la discusión con colegas y la puesta en práctica del MRU, se procederá a la actualización del Modelo de Madurez de SI, con el objetivo de

[1] El estadio de madurez "C" corresponde al nivel intermedio del Modelo de Madurez de Seguridad de la Información establecido durante TFE. Dicho Modelo consta de 6 niveles, denominados utilizando las letras A, B, C, D, E y F, donde A simboliza el nivel óptimo de mejora continua de Seguridad de la Información y F el nivel nulo de Seguridad de la Información.

[2] Los niveles "A" y "B" del Modelo de Madurez de Seguridad de la Información se encuentran conformados por requerimientos complejos que exceden significativamente al alcance de la norma ISO 27.001 y de las implementaciones de Seguridad de la Información del común de las organizaciones.

convertirlo en una metodología de referencia más adaptable y menos rígida para facilitar su compatibilidad con cualquier tipo de organización. Dichas modificaciones son complementarias al macroproceso de implementación ya que se enfocan principalmente en facilitar el camino que las organizaciones deben recorrer desde un mínimo o nulo nivel de SI hasta lograr alcanzar el estadio de madurez general "C".

Por último, el objetivo final del presente TFM radica en la generación de una versión superadora del MRU, que no solo extiende dicho Marco de Referencia, sino que también logra simplificarlo, aumentar su adaptabilidad, disminuir su rigidez y facilitar su implementación a través de la incorporación de nuevos componentes, secciones y metodologías. De esta forma, se logra facilitar el objetivo fundamental del MRU: guiar y apoyar a la organización antes, durante y después de la implementación de un Sistema de Mejora Continua en SI.

Palabras claves

Metodología, Seguridad de la Información, Buenas prácticas, Estándares Internacionales, Procesos de Negocio, Mejora Continua, Sinergia de Buenas Prácticas, Enfoque en el Negocio, Modelo de Madurez de Seguridad de la Información.

0.2 Índice de contenidos

[Página dejada en blanco intencionalmente]

1

Breve introducción al MRU[3]

Durante el año 2017, a raíz del TFE[4], se establecieron las bases primordiales y fundamentales del MRU. El mismo pretendió abordar la simplificación de la extensa complejidad que los especialistas en SI enfrentan a la hora de implementar diversos estándares y normas internacionales en la materia. La dificultad no solo se centra en la gran cantidad de material a analizar, sino principalmente en la existencia de duplicaciones, redundancias, divergencias tanto de criterios como de prioridades, y hasta contradicciones entre dichos estándares y normas internacionales. Por tal motivo, el MRU se ha enfocado específicamente en la centralización de dichos documentos en una única fuente complementada junto con un Modelo de Madurez que establezca el camino a seguir, permitiendo guiar de forma simple y efectiva a las organizaciones hacia la mejora continua en SI.

Para comenzar con el presente TFM debemos obligatoriamente realizar una breve recapitulación de los lineamientos del MRU que han sido desarrollados durante el TFE. De esta forma, se facilitará significativamente la comprensión por parte del lector, ya que los mismos configuran la base fundamental de todos los conceptos desarrollados dentro del presente trabajo. A su vez, complementariamente a la recapitulación se introducirán y detallarán las nuevas incorporaciones y modificaciones realizadas al MRU por el TFM.

[3] Marco de Referencia Unificado en Seguridad de la Información.
[4] Trabajo Final de Especialización. Disponible para descarga dentro del catálogo de la biblioteca digital de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires, click aquí.

1.1 ¿Que posibilita el MRU?

El MRU logra establecer una colección de buenas prácticas en un único marco de referencia, en otras palabras, centraliza y combina los lineamientos, controles, actividades, procesos y políticas detalladas en diversos estándares, normas, marcos de referencia y guías internacionales de SI. Esta centralización logra establecer una integración y complementación entre las diversas buenas prácticas que conforman el MRU, generando así una sinergia única entre estas. No obstante, el MRU no configura únicamente una mera colección de buenas prácticas. Estas han sido homogeneizadas en función de las siete guías estratégicas[5] del MRU (*Enfoque en el Negocio, Mejora Continua, Involucramiento del Recurso Humano, Difusión & Entrenamiento, Calidad, Procesos de Negocio y Mejora Continua*). Este proceso de homogeneización se centra en integrar las duplicaciones, eliminar las omisiones y evitar las posibles contradicciones entre los distintos estándares, normas y marcos de referencia de SI considerados por el MRU.

El MRU logra a su vez establecer una guía de implementación de dicha colección de buenas prácticas. Esta guía corresponde a una metodología destinada a facilitar el camino a recorrer durante la implementación de sus requerimientos por parte de las organizaciones: el *Modelo de Madurez de SI* (en adelante, MMSI). Dicho Modelo de Madurez clasifica en 6 niveles diferentes la colección completa de buenas prácticas del MRU. De esta forma, cada organización podrá identificar su situación actual en cuanto a SI y evaluar la misma contra los distintos estadios de madurez para así conocer tanto su posición dentro del Modelo de Madurez como el camino a recorrer para alcanzar su nivel de madurez futuro deseado. Así es como el MRU logra adaptarse a cada situación individual, ya que el estadio de madurez objetivo es decisión exclusiva de cada organización. Dicha decisión deberá corresponder al estadio de madurez de SI que la organización considera óptimo y adecuado para sí misma, debido a que el objetivo ulterior del MRU no consiste en proteger en forma extensa todos los activos de información de la

[5] Establecidas durante el Trabajo Final de Especialización, favor de referirse a la sección 2 de dicho trabajo para mayor información.

organización utilizando el máximo posible de recursos, sino que se basa en un análisis estratégico de riesgos. De esta forma, la organización logrará gestionar sus riesgos en forma efectiva y, a su vez, logrará disminuirlos a los niveles que considera aceptables, obteniendo así su nivel de SI apropiado adaptado a sus propias necesidades y a la naturaleza de su negocio.

El tercer logro del MRU radica principalmente en el diseño de un proceso de implementación de sus requerimientos. Dicho proceso forma parte del TFM (favor de referirse al capítulo 3 del presente trabajo) y pretende facilitar la utilización del Modelo de Madurez para la selección de las buenas prácticas de la colección del MRU por parte de los profesionales de SI. Este proceso conforma un macroproceso genérico capaz de moldearse a las necesidades de cada organización gracias a su alto nivel de abstracción y, principalmente, debido a su enfoque de macro actividades[6]. Basado en la lógica de procesos de negocio, en los lineamientos de la norma ISO 27.003:2010[7] y en la integración entre el Modelo de Madurez de SI y la colección de buenas prácticas del MRU, el macroproceso de implementación logra simplificar y agilizar las implementaciones de los requerimientos de SI del MRU.

En función de lo detallado anteriormente, podemos concluir que la misión del MRU consiste en: "*Convertirse en el marco de referencia más completo y a la vez más simple de implementar en la materia*" [2] con el objetivo de "*realizar un aporte al mundo de la SI*" [2]. Para ello, permite "*a las organizaciones alcanzar la Mejora Continua en SI a través del establecimiento de los procesos y buenas prácticas requeridas, de los controles necesarios* […] *y de las soluciones de seguridad que permitan optimizar la efectividad de los objetivos estratégicos de las organizaciones del siglo XXI*" [2] y, a su vez, la disminución

[6] El enfoque de macroactividades se distingue principalmente por su alto nivel de abstracción y por detallar múltiples actividades estratégicas cuya "*bajada a tierra*" queda a criterio de cada organización.
[7] El macroproceso se ha construido tomando a consideración las buenas prácticas identificadas tanto en la ISO 27.003:2010 como su norma sucesora, la 27.003:2017 (incorporando únicamente los lineamientos de su borrador general de 2016 dentro del presente trabajo).

hasta un nivel aceptable por la organización de "*los riesgos de seguridad asociados al activo más preciado que poseen: su información*" [2].

En definitiva, el MRU brinda un marco de referencia holístico[8] y práctico para todos aquellos que deseen alcanzar un estadio de madurez de mejora continua en materia de SI. A su vez, logra evitar que las organizaciones no aborden la SI desde todos los ángulos necesarios, logrando así un enfoque equilibrado de SI para la organización tomando en cuenta todos los requerimientos tanto técnicos y tecnológicos como de gestión y de gobierno de la SI. Dicho equilibrio demuestra claramente que el MRU se encuentra fundamentalmente orientado al negocio (específicamente a la alta dirección de las organizaciones) y a generar valor para la organización evitando la destrucción y preservando el valor que la misma genera a lo largo del tiempo.

1.2 ¿Por qué es necesario un marco de referencia holístico?

El MRU conforma un marco de referencia holístico[9] conforme a que pretende alcanzar a las normas y estándares más significativos en la materia. De esta forma, logra establecer un alcance global de la SI incorporando, integrando y combinando dentro de un Modelo de Madurez diversos aspectos técnicos (por ejemplo: seguridad de redes, algoritmos criptográficos, entre otros aspectos), tecnológicos (por ejemplo: disponibilidad del centro de cómputos, ciclo de vida de los sistemas de información, entre otros aspectos) y de gestión (por ejemplo: gestión de riesgos, procesos de negocio, gobierno de SI, entre otros aspectos) con el objetivo de crear una sinergia única entre estos. Dentro del campo de la SI existe una variada oferta de estándares y normas en la materia enfocados en diversos aspectos, desde los que ven a la seguridad desde un punto de vista puramente técnico hasta los que atacan la seguridad exclusivamente desde el panorama de su gestión estratégica y, a su vez, aquellos que combinan con mayor o menor éxito

[8] Holístico: "*Del todo o que considera algo como un todo*"[28]. Hace referencia al alcance del presente trabajo que, pretende alcanzar a las normas más significativas en la materia.
[9] Holístico: "*Del todo o que considera algo como un todo*"[28]. Hace referencia al alcance del presente trabajo que, pretende alcanzar a las normas más significativas en la materia.

estos dos mundos. El MRU conforma un marco de referencia holístico no solo porque pretende alcanzar a las normas y estándares más significativos sino también debido a su enfoque integrador tanto del mundo técnico de Seguridad como del mundo de la gestión de la SI.

A la hora de implementar "*frameworks*", los profesionales de seguridad se encuentran con la necesidad de estudiar múltiples y diversos estándares, y también de analizar la forma en que estos se complementan, contradicen o generan redundancias entre sí. A su vez, dichos profesionales deberán planificar que lineamientos de los estándares que han analizado implementarán en sus organizaciones y de qué manera llevarán adelante dicha implementación, lo que genera una significativa complejidad a derribar por parte de los profesionales de SI. Dicha complejidad es la que el MRU logra simplificar, al ofrecer un enfoque de seguridad:

- Balanceado entre los mundos técnico y no técnico de seguridad. Estableciendo mecanismos de Gobierno de Seguridad que logren integrar a la organización como un todo en materia de SI y asegurándose que la SI de la organización sea atacada desde todos sus frentes.
- Planificado a través del modelo de Madurez de SI, el cual facilita la planificación e implementación de las acciones de SI por parte de la alta dirección (Gerentes de SI, comúnmente denominados CISOs) o de consultores de Seguridad.
- Global al ser una colección de buenas prácticas en un único marco de referencia, al intentar reflejar el estado del arte en materia de SI.

De esta forma, el MRU logra satisfactoriamente convertirse en una guía dentro de la complejidad del mundo de la SI.

1.3 ¿Cómo surgió el MRU?

La idea del MRU nació a raíz de diversas dificultades encontradas durante la implementación de un complejo proyecto de SI. Dicho proyecto poseía el ambicioso

alcance de diseñar una política de seguridad que logrará abarcar y combinar una gran cantidad de normas, estándares, marcos de referencia y guías en la materia, con el objetivo de generar un "*best of breed*"[10] para la SI de las organizaciones.

El proyecto se convirtió en una tarea significativamente ardua, laboriosa y compleja que sin duda alguna estaba condenada al fracaso. Esto último se debe a que el objetivo final del proyecto se basaba en la conformación de una gran política de SI que, más pronto que tarde, comenzó a adquirir dimensiones significativas que dificultaban no solo su lectura, pero también su entendimiento inclusive por lectores experimentados en la temática. Más adelante, la complejidad obligo a virar el enfoque del proyecto de diseño de una gran política a la producción de una serie de políticas específicas en diversas áreas de seguridad que alivianaran la carga de contenido de la política central. No obstante, la complejidad continuaba existiendo, solo que ahora se encontraba clasificada dentro de diversos grupos temáticos de Seguridad representados por las diferentes políticas del proyecto. Fue entonces cuando se tomó la decisión de incorporar la lógica de los procesos de negocio al proyecto. Así, las 25 políticas de SI que combinaban e integraban múltiples estándares fueron siendo traducidas a procesos de negocio, lo que simplifico y facilito su implementación debido a que los procesos permitieron el entendimiento por parte del lector no técnico, la documentación de las responsabilidades y la simplificación de las necesidades de capacitación y de gestión del cambio. De esta forma, se logró efectivamente concretar el objetivo de creación de un "*best of breed*"[6] de SI.

La significativa complejidad del proyecto consistió en la inexistencia de un elemento intermedio que facilitara la centralización y clasificación de buenas prácticas, algo que debió ser realizado previo a su incorporación dentro de las políticas de seguridad del proyecto. De existir un marco de referencia que les evitara a los profesionales de seguridad la necesidad no solo de estudiar múltiples y diversos estándares en la materia sino también de analizar la forma en que estos se complementan, contradicen o generan

[10] Hace referencia a "*Cualquier ítem o producto considerado el mejor en su tipo*" [17] al combinar e integrar todos los elementos únicos o buenas prácticas de varios productos.

redundancias entre sí, la complejidad del proyecto podría haberse disminuido significativamente. Fue en ese momento, cuando surgió la idea de realizar un trabajo más estratégico que incrementara el nivel de abstracción, con el fin de diseñar un marco de referencia que hiciera la vida de los profesionales de SI más sencilla y diera vida a ese elemento intermedio faltante.

El propósito fundamental del MRU radica en facilitar y mejorar la compleja experiencia a la que todos aquellos profesionales de SI se enfrentan a la hora de llevar a la práctica implementaciones de seguridad ad-hoc dentro de sus organizaciones. Por lo que, el MRU, propone convertirse en una herramienta del profesional de seguridad que permita, a través de la centralización de buenas prácticas y la incorporación de complementos destinados a facilitar el camino a recorrer durante las implementaciones de seguridad, agilizar, simplificar y planificar su trabajo.

1.4 ¿A quién está dirigido?

El Marco de Referencia Unificado en SI está principalmente pensado para una implementación dentro de grandes organizaciones. Este es el motivo por el cual realiza un significativo hincapié tanto en mecanismos de gobierno, estrategia y de medición y evaluación de la SI como en políticas y procesos vinculados a la gestión estratégica de la misma, con el objetivo de atacar la complejidad de las grandes organizaciones. Este enfoque del MRU resulta excesivamente completo para pequeñas organizaciones, por lo que se recomienda que las mismas tomen los requerimientos del MRU a forma de guía y consulta enfocándose principalmente en los estadios de madurez "E" y "D"[11], añadiendo el nivel "C" para aquellas organizaciones consideradas de tamaño intermedio.

El MRU puede ser utilizado y aplicado por compañías públicas y privadas, instituciones y entes públicos, asociaciones sin fines de lucro y cualquier otro tipo de

[11] Dichos estadios de madurez corresponden a los niveles mínimos del Modelo de Madurez de Seguridad de la Información del MRU. Favor de referirse a la sección 2.3 del presente TFM para obtener mayor información sobre los niveles de madurez del MRU.

organización de gran tamaño que desee alcanzar un estadio de madurez de mejora continua en materia de SI.

Además de poseer un espacio de aplicación enfocado principalmente a organizaciones de gran envergadura, el MRU ofrece un enfoque estratégico y pragmático para todos aquellos que deseen alcanzar un estadio de madurez de mejora continua en materia de SI. Por lo que, el grupo de usuarios objetivo de este marco de referencia incluirá:

- CISOs o Gerentes de SI, los cuales podrán utilizar el MRU como herramienta estratégica para su gestión o en forma de guía y consulta para la confección de sus iniciativas y proyectos de seguridad.
- Consultores especializados en implementaciones o proyectos de SI, quienes podrán utilizar el MRU al momento de planificar y diseñar sus soluciones y arquitecturas de seguridad.
- A la comunidad, con el objetivo de que los profesionales de seguridad, investigadores o especialistas en el área tomen la idea que representa el MRU y puedan mejorarla y llevarla a la práctica en un futuro cercano.

1.5 ¿Cuáles son los componentes del MRU?

Desde su concepción dentro del TFE, el MRU poseía 2 grandes componentes principales: el *Sistema de Mejora Continua en SI*[12] (el sistema de gestión de SI basado en buenas prácticas que la organización deberá diseñar e implementar) y el *Modelo de Madurez de SI* (la herramienta del MRU que facilita la priorización de las buenas prácticas y encausa el camino que las organizaciones recorrerán en materia de SI). El presente TFM identifica un tercer componente, la *Colección de Buenas prácticas de SI*, e incorpora un cuarto: el *Macroproceso de implementación del Sistema de Mejora Continua en SI*. La ilustración 1.5.1 detalla estos cuatro componentes y la relación existente entre ellos. En

[12] El símil del MRU al "*SGSI: Sistema de Gestión de Seguridad de la Información*" [1] de la norma ISO 27.001.

dicha ilustración, puede fácilmente visualizarse que el Sistema de Mejora Continua en SI es alimentado por los restantes componentes. Esto último, se debe a que la organización diseñará su propio Sistema de Mejora Continua en función de las buenas prácticas que identifique necesarias para su naturaleza, la priorización que realice sobre dichas buenas prácticas basándose en su estadio de madurez objetivo y los lineamientos del proceso de implementación que considere necesarios.

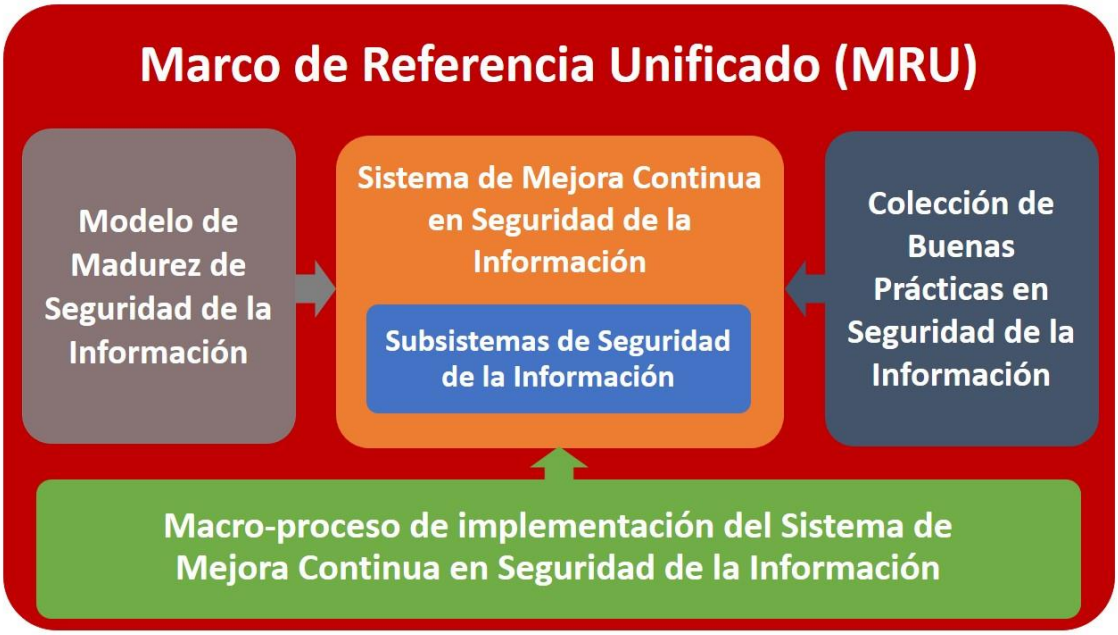

Ilustración 1.5.1: componentes del MRU.

En función de lo detallado anteriormente, se procederá a describir los detalles de cada uno de los cuatro componentes que conforman el MRU.

Sistema de Mejora Continua en SI
Definición
Es el Sistema de Gestión de SI que implementa el MRU, basándose en el reconocido "*SGSI*" [1] establecido por la norma ISO 27.001 [1]. No obstante, el Sistema de Mejora Continua contiene tanto un alcance como una profundidad significativamente superior al "*SGSI*" [1], ya que no se limita únicamente a los lineamientos de la norma ISO 27.001 [1] sino que va más allá, incorporando:

- Herramientas estratégicas de gobierno de SI.
- La lógica de los procesos de negocio.
- Mecanismos avanzados de gestión de riesgos de SI.
- Estadios de Madurez de la SI, complementarios al Modelo de Madurez de SI del MRU.
- Una visión holística de la SI.

A medida de la organización

Cada organización desarrollará su propio Sistema de Mejora Continua en SI, en función de:

1. Las buenas prácticas detalladas en el MRU que la organización identifique como necesarias. El Sistema de Mejora Continua en SI de la organización contendrá todos los requerimientos (controles, buenas prácticas, procesos, procedimientos, políticas y lineamientos) del MRU que se alinean tanto a la naturaleza como a las necesidades de la organización.
2. La priorización de la implementación de las buenas prácticas identificadas en función del estadio de madurez de seguridad objetivo de la organización. El objetivo del Modelo de Madurez del MRU consiste en permitirle a la organización ir adicionando las buenas prácticas en forma simple y estructurada a lo largo del tiempo en función de un nivel de dificultad de implementación creciente. De esta forma, la organización ira moldeando su camino hacia su estadio de madurez futuro objetivo.
3. Los lineamientos del proceso de implementación que la organización identifique como necesarios para la construcción de las políticas, procesos, mecanismos y lineamientos de seguridad que conformarán el Sistema de Mejora Continua en SI de la organización.

Estos tres lineamientos conforman una de las principales guías incorporadas dentro del macroproceso de implementación del Sistema de Mejora Continua en SI.

Subsistemas de Seguridad de la Información

El Sistema de Mejora Continua en SI es desarrollado por el MRU a través de un conjunto de 9 Subsistemas, los cuales engloban las diversas ramas y temáticas de la SI. De esta forma, los requerimientos del estado del arte en Seguridad, contenidos por el MRU, se encuentran agrupados y clasificados dentro de los

siguientes nueve Subsistemas, que podrán visualizarse fácilmente dentro de la ilustración incluida a continuación.

Ilustración 1.5.2: Subsistemas de Seguridad de la Información.

El desarrollo en detalle de Subsistemas de Seguridad podrá encontrarse tanto en el Anexo del TFE (donde se establecen los Subsistemas piloto del MRU: Gobierno de Seguridad y Lineamientos de Seguridad) como, a su vez, en el anexo I del presente TFM.

Cada uno de los Subsistemas de SI contiene una serie de requerimientos a cumplir basados en controles, protocolos, reglas, procesos, metodologías, guías y formas de organización del flujo de trabajo de Seguridad. Para facilitar su comprensión por parte del lector, los requerimientos serán a su vez clasificados en diversas subcategorías dentro de los Subsistemas de SI. La descripción y desglose de dichas subcategorías podrán encontrarse en forma completa en el anexo I del presente trabajo.

Propósito

El Sistema de Mejora Continua en SI, al ser holístico y lograr una extensa cobertura de las normas y estándares internacionales más relevantes en la materia, brinda a las organizaciones la posibilidad de responder de forma

pragmática a la evolución de la tecnología y a la constante mutación de sus riesgos de seguridad. De esta forma, logra que las organizaciones:

- Obtengan una clara guía de apoyo a sus implementaciones de seguridad, a través de una serie de requerimientos de SI orientados al negocio y, clasificados en función del Modelo de Madurez del MRU.
- Identifiquen e integren al Sistema de Mejora Continua en SI los distintos requerimientos legales, regulatorios, estatutarios, contractuales y de mercado que deben cumplir.
- Utilicen una metodología simple y pragmática que los acompañe en el tiempo a través de sus implementaciones de SI.

Modelo de Madurez de Seguridad de la Información

Definición

El segundo componente del MRU, consiste en el Modelo de Madurez de SI. El objetivo de este radica en proveer una guía a las organizaciones para la implementación de los requerimientos del MRU. Dicha guía acompañará a las organizaciones desde un punto de partida básico de seguridad hasta el logro de la mejora continua en SI.

Para lograr este objetivo, el Modelo de Madurez del MRU clasifica todos sus requerimientos de seguridad en función de 6 estadios de madurez (denominados con las letras “F”, “E”, “D”, “C”, “B” y “A”). Dichos estadios se encuentran ordenados en un nivel creciente de madurez en cuanto a su complejidad de implementación y de gestión de los requerimientos de SI que contiene cada estadio. Cabe resaltar, que en principio el TFE estableció la condición de que cada nivel requiere de la implementación de sus requerimientos específicos y de los requerimientos de todos los niveles inferiores a éste, para poder declarar conformidad con dicho estadio de madurez. No obstante, dentro de la sección 2.5 del TFM, abordaremos una nueva perspectiva sobre la construcción de los distintos estadios de madurez de SI.

El Modelo de Madurez de SI ha sido específicamente diseñado para guiar el establecimiento de un Sistema de Mejora Continua en SI desde la “*ignorancia feliz*” [18] hacia la mejora continua en SI. De esta forma el logro de la implementación en forma completa del Sistema de Mejora Continua en SI por

parte de una organización se ve facilitado y simplificado significativamente, ya que solo se debe seguir los pasos establecidos en dicho modelo, implementando en forma gradual y priorizando los requerimientos del MRU. El Modelo de Madurez de SI permite comenzar con una sólida base general de seguridad para luego iniciar a afinar, extender y complejizar la misma, con el objetivo final de lograr la mejora continua en SI.

Estructura base del Modelo de Madurez

El TFE estableció la estructura general y la clasificación de los distintos niveles del Modelo de Madurez de SI. Sin embargo, el presente trabajo realiza ciertas enmiendas y modificaciones al mismo, aunque mantiene su estructura general. Se incluye a continuación una ilustración que detalla la composición general del Modelo de Madurez de SI[13] introducido durante la realización del TFE.

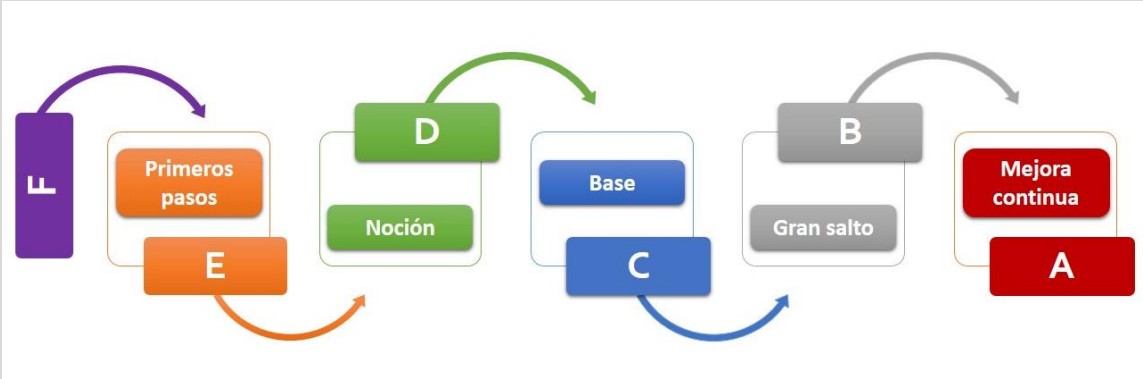

Ilustración 1.5.3: estadios de madurez de Seguridad de la Información.

El camino hacia la mejora continua que las distintas organizaciones deberán recorrer es desafiante y complejo. Por este motivo, el MRU establece el Modelo de Madurez de SI incorporando seis estadios de madurez: el primero simboliza la falta total de controles o lineamientos de seguridad (el nivel "F"), los cuatro siguientes niveles implementarán parcialmente de forma creciente los requerimientos del MRU, mientras que el último nivel contiene todos los requerimientos necesarios para implementar el Sistema de Mejora Continua en SI en forma completa. De esta forma, gracias al Modelo de Madurez de SI, se simplifica significativamente el recorrido que las organizaciones deberán afrontar

[13] Existen 6 estadios de madurez MRU, cada uno de ellos con sus respectivos requerimientos a cumplir en función de una complejidad ascendente.

desde un estadio de "*ignorancia feliz*" [18], hasta lograr optimizarlo alcanzando la mejora continua en SI.

Propósito

El Modelo de Madurez de SI conforma el objetivo primordial del MRU, al ser una guía holista y práctica para que cualquier tipo de organización pueda navegar de forma simple desde los niveles iniciales, hasta alcanzar la mejora continua en SI. Su objetivo es guiar y apoyar a la organización antes, durante y después de la implementación del Sistema de Mejora Continua en SI. El desarrollo en detalle de este podrá de encontrarse en el capítulo 4 del TFE y sus consecuentes enmiendas dentro de la sección 2.3 del presente TFM.

Colección de Buenas prácticas en SI

Definición

Es el componente que engloba a todas las buenas prácticas incluidas dentro del MRU. Detalla todos los requerimientos, lineamientos, controles, políticas y procesos de los diversos estándares y normas de SI analizadas por el MRU.

Este componente detalla las buenas prácticas en SI a través de:

- El establecimiento de en un formato homogeneizado de buenas prácticas para facilitar la búsqueda e identificación de éstas por parte de los profesionales de seguridad.
- La clasificación de las buenas prácticas dentro de los Subsistemas de SI.
- Su forma de catalogar las buenas prácticas en función de los estadios de madurez del MRU.

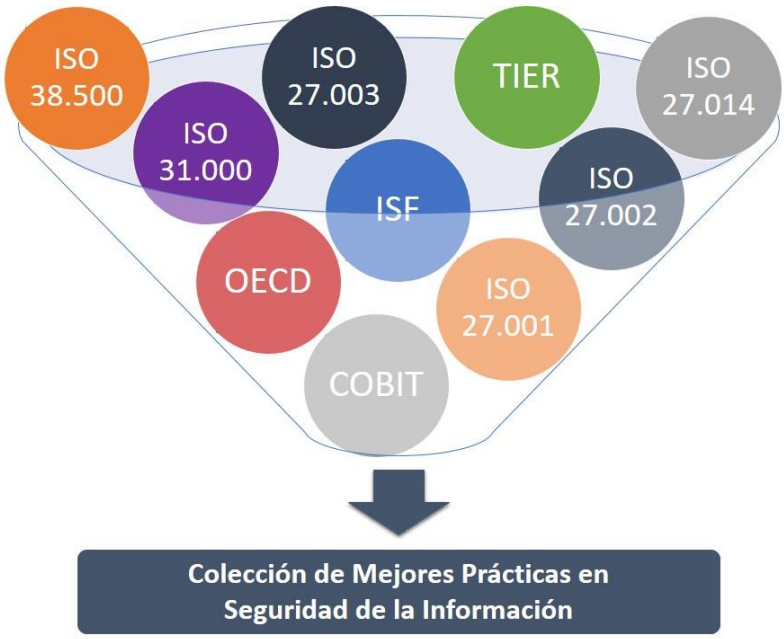

Ilustración 1.5.4: listado de algunas de las buenas prácticas que conforman la colección del MRU[14].

Propósito
La colección de buenas prácticas corresponde a un componente identificado dentro del TFM con el objetivo de facilitar la comprensión del lector tanto de la utilidad del MRU como de su mecanismo de uso. Su objetivo principal radica en ser utilizado por los profesionales de SI para identificar las buenas prácticas que más se adapten a la naturaleza de su organización en función de sus necesidades y su estadio de madurez objetivo.

Macroproceso de Implementación del Sistema de Mejora Continua
Definición
Conforma el cuarto componente del MRU, el cual fue adicionado durante el desarrollo del presente TFM. Basado en la lógica de procesos de negocio, consiste en un proceso estratégico de alto nivel (macroproceso) que identifica y

[14] Aclaración de las siglas detalladas en la ilustración 1.5.4. ISO: Organización Internacional de Estandarización, OECD: Organización para la Cooperación y el Desarrollo Económico, ISF: Foro de Seguridad de la Información, TIER: Estándar de clasificación TIER de centros de cómputos establecido por el Uptime Institute y COBIT: Objetivos de Control para Información y las Tecnologías relacionadas.

describe los procesos y actividades estratégicas que deben desarrollarse durante la implementación del Sistema de Mejora Continua en SI. De esta forma simplifica el trabajo de los profesionales de seguridad a la hora de diseñar el proyecto de adhesión al MRU.

Propósito
Proveer una guía y apoyo a los profesionales de seguridad durante: ▪ La identificación de las buenas prácticas que logran una combinación perfecta con la naturaleza y las necesidades de la organización. ▪ El diseño e implementación del Sistema de Mejora Continua de SI específico para la organización. ▪ El diseño e implementación de mejoras al Sistema de Mejora Continua de SI de la organización, con el objetivo de realizar un salto en los estadios de madurez del MRU.

1.6 ¿Qué es la documentación fuente del MRU?

Al ser una colección de buenas prácticas, el MRU basa su construcción en la consulta y análisis de diversos estándares, normas, marcos teóricos, manuales y guías internacionales y nacionales de SI. Es por este motivo que surge la necesidad de establecer un concepto cuya definición represente a todos los documentos de seguridad que han sido considerados durante la concepción del MRU. Es aquí donde entra en juego el concepto de documentación fuente, el cual efectivamente engloba a todos los estándares, normas, marcos teóricos, manuales y guías internacionales de SI que el MRU se ha propuesto centralizar y consolidar dentro de su colección de buenas prácticas. De esta forma podemos establecer que el MRU centraliza, clasifica, relaciona y crea una complementación e integración única entre todos los requerimientos individuales de cada norma o estándar que compone su documentación fuente, con el objetivo de facilitar las implementaciones de SI por parte de cualquier tipo de organización. Cabe resaltar, que el MRU no engloba a todos los estándares, normas, marcos teóricos, manuales y guías internacionales existentes de SI, sino que considera solo a algunos de estos documentos en función del criterio establecido por el autor. El criterio de selección de la

documentación fuente fue explicado en detalle dentro de la sección 1.4 del TFE ("*Criterio de selección de normas y estándares*" [2]), favor de referirse a dicha sección.

El detalle completo de la documentación fuente utilizada por el MRU puede encontrarse tanto en la sección de bibliografía del TFE como en la sección de bibliografía del presente trabajo. Para facilitar la tarea del lector, se incluye a continuación una ilustración que realiza un paneo general de toda la documentación fuente identificada por el MRU. Se debe tomar en cuenta que parte de la documentación fuente contenida en la ilustración ha sido incluida dentro de los próximos pasos a seguir en la confección del MRU (favor de referirse al capítulo 4 del presente trabajo), por lo que podría no encontrarse incluida dentro de la versión del marco de referencia producido por el presente trabajo.

Entre los estándares, marcos teóricos, normas, guías y marcos de referencia internacionales considerados[15], se encuentran los siguientes:

Ilustración 1.6.1: documentación fuente identificada por el MRU.

[15] Podrá encontrarse el detalle completo de la documentación fuente en la sección bibliográfica tanto del presente trabajo como del Trabajo Final de Especialización.

La documentación fuente incluida dentro de recuadros en el borde inferior de la ilustración 1.6.1 hace referencia a:

- Las normas ISO 27.003 [19], las publicaciones especiales del NIST SP-800[16], los marcos de trabajo ISF [4] y COBIT [5], la norma ISO 27.001 [1] y, por último, la norma ISO 27.002 [14]. Dicha documentación fuente ha influido a varios Subsistemas de Seguridad, lo cual es representado a través de su agrupamiento dentro del recuadro que las contiene. No se identifican las vinculaciones particulares a cada Subsistema ya esto podría fácilmente confundir al lector.
- La norma ISO 27.003 [20], se encuentra a su vez estrechamente vinculada al macroproceso de implementación del Sistema de Mejora Continua en SI. Ese es el motivo por el cual se la representa también dentro de otro recuadro.

La construcción de los requerimientos del MRU incluyo a su vez, en un pequeño porcentaje, la incorporación de experiencias profesionales tanto propias como de colegas, además de ciertos cambios y lineamientos introducidos por el autor. No obstante, más del 90% de los requerimientos del MRU se basan exclusivamente en las normas y estándares incluidos dentro de la documentación fuente (la cual puede observarse en la ilustración 1.6.1).

1.7 ¿Qué modificaciones al MRU incorpora el presente trabajo?

El objetivo principal del presente TFM no recae únicamente en completar el MRU hasta su nivel "C", sino también en mejorarlo a través de la incorporación de nuevas metodologías y complementos que auxiliarán a los profesionales de seguridad durante la implementación de los requerimientos del Sistema de Mejora Continua en SI. Se incluyen a continuación un detalle de todas las modificaciones realizadas al MRU por el presente trabajo:

[16] Las mismas fueron incluidas como uno de los próximos pasos para el desarrollo del MRU, quedando fuera del alcance del presente TFM.

- Mejoras a la versión piloto del MRU: se procedió a realizar una referencia cruzada entre las normas ISO 27.001 [1], ISO 27.002 [14] e ISO 31.000 [6] y el MRU, lo que precipito el diseño de ciertas mejoras a los Subsistemas de Seguridad pilotos establecidos durante el TFE. De esta forma, el MRU actualmente logra implementar todos los requerimientos detallados por estas tres normas ISO. Las mejoras podrán encontrarse dentro del Anexo II del presente trabajo.
- Macroproceso de implementación del Sistema de Mejora Continua en SI: se confecciono un nuevo componente del MRU para paliar la complejidad que los profesionales de seguridad abordarán durante la implementación de los requerimientos del MRU y el diseño del Sistema de Mejora Continua en SI.
- Incorporación de las Capas de Seguridad del MRU: se incorporan con el objetivo de facilitar la visualización de la "bajada a tierra" de la estrategia del MRU (favor de referirse al capítulo 2 del TFE) dentro del Modelo de Madurez de SI.
- Disminución de la rigidez del Modelo de Madurez: con el objetivo de flexibilizar la adaptación de la organización a los requerimientos de cada estadio de madurez del MRU y, en consecuencia, simplificar y agilizar el camino que deberán recorrer en materia de SI.
- Incorporación de buenas prácticas: con el objetivo de completar todos los Subsistemas de Seguridad del MRU, por lo menos hasta sus correspondientes estadios de madurez "C".

[Página dejada en blanco intencionalmente]

2

Cimientos del MRU

El diseño tanto de los requerimientos como de los Subsistemas de Seguridad y de los diferentes estadios de madurez del MRU responden a una cierta lógica. Dicha lógica se desprende directamente de la Estrategia del MRU, cuyos siete componentes[17] han sido establecidos durante el TFE. Dentro del presente capítulo abordaremos el porqué de la existencia de esta lógica que hay detrás del MRU y, a su vez, analizaremos en detalle su interrelación con los componentes del MRU.

2.1 Ordenamiento de requerimientos[18]

Lo primero que debemos analizar, para comprender la lógica existente detrás del MRU, consiste en una de las grandes diferencias que el MRU posee con los demás estándares y normas de SI. En contraste con todos los documentos que componen la documentación fuente (por ejemplo: la norma ISO 27.001 [3] o el marco de trabajo COBIT5 [5]), el orden de los requerimientos del MRU refleja no solo su importancia, sino a su vez su complejidad de implementación. Esto último se debe a que cada uno de los requerimientos del MRU se encuentran clasificados y agrupados en función de los lineamientos de cada uno de los estadios de madurez de Seguridad del MRU. De esta

[17] Favor de referirse al capítulo 2 del Trabajo Final de Especialización para mayor detalle e información.
[18] Los requerimientos del MRU conforman el elemento de menor jerarquía y fundamental del MRU. Son aquellos que conforman los Subsistemas, Áreas y Dominios de Seguridad de la Información. A su vez, representan todo control, proceso, política, medida, lineamiento, procedimiento, buena práctica o acción individual de Seguridad de la Información delineada dentro del MRU.

forma, el ordenamiento de los requerimientos del MRU responderá a la lógica del Modelo de Madurez de SI: detallándose en primera instancia las principales bases en seguridad y luego en forma de complejidad creciente los diversos requerimientos en pos de alcanzar la mejora continua en SI.

Este es el motivo por el cual cada uno de los Subsistemas de Seguridad contendrá sus requerimientos clasificados y ordenados en función de un nivel creciente de complejidad de implementación. Por lo que, cada subsistema comenzará a detallar sus requerimientos desde el estadio de madurez mínimo (correspondiente al nivel "E") y cuando estos se agoten continuará con los estadios intermedios (aquellos denominados "D", "C" y "B" respectivamente) hasta finalizar con el máximo nivel de seguridad (correspondiente al estadio de madurez "A").

¿Qué gobierna la lógica del Modelo de Madurez de SI? La misma que rige la Colección de Buenas prácticas del MRU. Dicha lógica, sin duda alguna ha moldeado el proceso de identificación y análisis de cada uno de los documentos que pudieran formar parte su documentación fuente. En función de esta lógica, se le ha dado mayor importancia a la incorporación de ciertos estándares y normas de seguridad sobre otros documentos similares y, más aun, sobre ciertas secciones de estos. Tal como sucede con el Modelo de Madurez y la Colección de Buenas prácticas, todos los componentes del MRU se encuentran entrelazados y gobernados por la misma lógica: la Estrategia del MRU.

El MRU basa en forma completa el desarrollo tanto de su estructura como de sus requerimientos individuales en el cumplimiento de sus siete principios estratégicos[19] ("*Enfoque en el negocio, Involucramiento del Recurso Humano, Procesos de negocios, Calidad, Mejora Continua, Buenas prácticas y Difusión & Entrenamiento*" [2]). De esta forma, logra "*llevar a la práctica la Estrategia del MRU*" [2] a través del Sistema de Mejora Continua en SI, "*el cual implementa el total de los requerimientos*" [2] de seguridad "*necesarios para alcanzar el estadio de madurez de mejora continua en SI*" [2].

[19] Favor de referirse al capítulo 2 del Trabajo Final de Especialización para mayor detalle e información.

El TFM pretende ahondar en el desarrollo de la Estrategia del MRU. Si bien la misma fue establecida durante la realización del TFE, el presente trabajo incorporará una visión más detallada de la Estrategia llevada adelante por el MRU, al profundizar tanto en sus características y componentes como en su estrecha interrelación con el Modelo de Madurez de SI.

2.2 Visión estratégica de la Seguridad de la Información

La adopción e implementación del MRU no es algo que la organización debe tomar a la ligera. Si bien los primeros estadios de madurez de seguridad podrán parecer sencillos de implementar a primera vista, la dificultad y complejidad a enfrentar, por parte de la organización, incrementan exponencialmente a media que se navegue en dirección al estadio máximo de madurez de seguridad. Previo al comienzo de la implementación del MRU, la organización deberá encontrarse perfectamente alineada y enfocada en el éxito de este proyecto desde su dirección ejecutiva y órgano de gobierno corporativo (de existir) hasta los eslabones de menor jerarquía de su estructura. De lo contrario, poseerá una visión parcial y sesgada de la SI desde el inicio del proyecto y carecerá tanto de la voluntad, intención y/o recursos necesarios para una implementación exitosa de alguna de las versiones del Sistema de Mejora Continua en SI. Abordaremos en mayor detalle esta perspectiva de implementación práctica dentro del capítulo 3 del presente trabajo.

Tal como detalla la norma ISO 27.001 [1], la adopción del Sistema de Mejora Continua en SI "*es una decisión estratégica de la organización.*" [1]. El diseño, "*establecimiento y la implementación del*" [1] Sistema de Mejora Continua en SI de la organización deberá encontrarse "*influenciado por sus necesidades, objetivos, requisitos de seguridad, sus procesos, estructura y su tamaño*" [1]. A su vez, "*se espera que estos factores cambien a lo largo del tiempo*" [1]. En otras palabras, el Sistema de Mejora Continua de la organización deberá encontrarse perfectamente alineado en todo momento a su naturaleza. Logrando así que el mismo se amolde e integre tanto a la estructura [1] como a los procesos [1] y al marco de gobierno [2], para así de esta manera

lograr formar parte de e integrarse completamente con la organización. Es por este motivo que todas las implementaciones del MRU serán diferentes, ya que cada organización moldeará el Sistema de Mejora Continua en función de sus propias necesidades.

Aquí es donde la singularidad del MRU juega un papel que marca la diferencia entre la gran variedad de normas y estándares existentes. La introducción del ordenamiento de requerimientos en función de los estadios de madurez permite a las organizaciones identificar fácilmente las buenas prácticas que mejor combinan con su naturaleza, agilizar la implementación de estas y simplificar el camino a recorrer proveyendo hitos y paradas intermedias entre el estadio de madurez actual de la organización y su estadio de madurez futuro objetivo.

2.3 Mejoras introducidas al Modelo de Madurez del MRU

Durante la realización del presente TFM se han introducido ciertas mejoras y enmiendas al Modelo de Madurez de SI. Las mismas se han basado en el propósito de:

- Brindar una mayor flexibilidad a las implementaciones particulares del MRU.
- Incorporar ciertos cambios a los lineamientos específicos de cada uno de los niveles de madurez.
- Homogeneizar los lineamientos de cada estadio de madurez con los requerimientos diseñados durante el TFM.

Realizando una breve recapitulación de su estructura, el TFE estableció la lógica del Modelo de Madurez basada en seis estadios de madurez de SI (favor de referirse a la ilustración 2.3.1): el primero conforma la inexistencia de controles de seguridad (“F”), los siguientes cuatro estadios implementan parcialmente y de forma creciente los requerimientos del MRU, mientras que el último nivel (“A”) contendrá todos los requerimientos necesarios para implementar el Sistema de Mejora Continua en SI en forma completa. De esta forma, gracias al Modelo de Madurez del MRU, se simplifica

significativamente el recorrido que las organizaciones deberán afrontar desde un estadio de "*ignorancia feliz*" [18], hasta lograr optimizarlo alcanzando la mejora continua en SI.

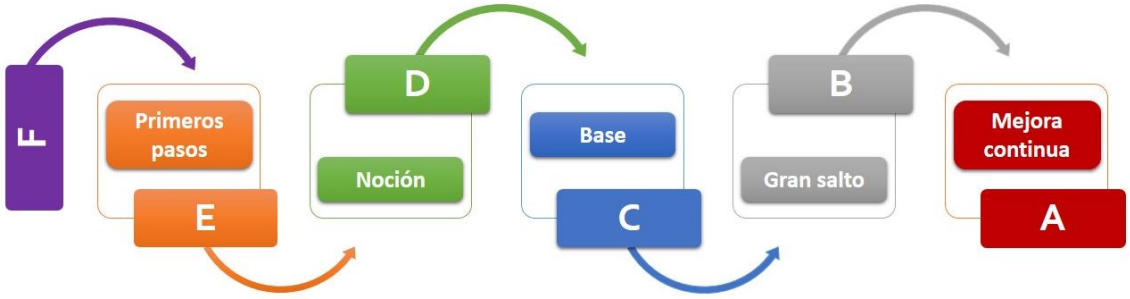

Ilustración 2.3.1: Estadios de madurez de Seguridad de la Información.

A su vez, el TFE, dividió a los estadios de madurez del MRU en función de una lógica de cuatro etapas de madurez [2]. El TFM toma estas cuatro etapas e incorpora ciertos cambios y modificaciones a las mismas. Por lo que dichas etapas de madurez quedan conformadas de la siguiente forma:

- "*Ignorancia feliz*" [18]: etapa de madurez referida a todas aquellas organizaciones que no logran alcanzar el estadio de madurez "E" [2]. En otras palabras, engloba a todas aquellas organizaciones que no logran cumplir con los requerimientos mínimos de SI del MRU, por lo que viven dentro de su "*ignorancia feliz*" [18] [2]. El MRU las guiará en el camino que deberán emprender a través de los restantes niveles de madurez hasta alcanzar la mejora continua en SI [2].

- Noción de SI: etapa de madurez que comprende los estadios "E" y "D" [2]. Se centra en la "*bajada a tierra*" del primer paso de la Estrategia del MRU: los controles generales de seguridad. De esta forma, logra fortalecer los puntos primordiales y básicos de SI de la organización:
  - **Estadio de Madurez "E":** logra establecer de forma completa el relevamiento e identificación de los activos de información de la organización. A su vez, establece las bases para su gestión que será complementada por los requerimientos subsiguientes de los estadios "D" y "C". De esta forma, logra

sentar la base para una gestión de riesgos eficaz, ya que sin conocer los activos de información no nos será posible gestionar sus riegos. Aquí se diseñará e implementará el perímetro de seguridad física de la organización (el cual brindará uno de los resultados más visibles para la dirección ejecutiva, lo que colaborará en transmitirles la justificación de la inversión en SI) y establecerá una figura responsable de la SI de la organización (que más adelante podremos denominar como CISO). El nivel de madurez "E" constituye los primeros pasos de la organización hacia la mejora continua, simbolizado por el MRU al mantener a flote la SI de la organización.

- **Estadio de Madurez "D":** se centra en la gestión de riesgos y en la complementación de los controles básicos de seguridad. Dentro de este estadio de madurez se iniciarán las primeras acciones de concientización y capacitación en la temática, se establecerá el rol de CISO (punto primordial para la implementación exitosa de los estadios superiores) y se delinearán los lineamientos para una correcta gestión de los accesos a los activos de información identificados en el nivel de madurez inferior (lo que incluye una gestión de la identidad de los usuarios con dichos accesos) [2]. De esta forma se logra establecer una noción de SI dentro de la organización, simbolizado por el MRU como una lista de verificación de controles generales y primordiales de seguridad.

- Base de SI: etapa de madurez referida al nivel "C" [2]. Esta etapa se centra en la implementación de todos los requerimientos base de SI, tomando como punto de partida lo implementado en los estadios anteriores. Configura el estadio más común en el que encontraremos a la gran mayoría de organizaciones. Es por este motivo, que el estadio "C" requiere de la implementación de la norma ISO 27.001 [1], ya que la misma contiene todos los requerimientos básicos y generales de seguridad que un gran número de organizaciones implementa y, a su vez, configura el estándar de seguridad que posee mayor imagen y conocimiento público. Esta etapa pretende establecer una

base común en Seguridad (simbolizado por el MRU al plantar la semilla de la mejora continua), requiriendo:

- La implementación de un Gobierno de SI.
- La gestión por procesos de todas las actividades de la organización vinculadas a la Seguridad.
- Diferentes autoridades de SI específicamente enfocadas en las actividades del día a día de seguridad (actividades vinculadas a la gestión de incidentes, continuidad del negocio, entre otras) y en actividades futuras de visión de largo plazo (mejora continua, gestión por procesos, proyectos de mejora e innovación en el largo plazo, entre otras).
- El diseño e implementación de un programa de capacitación continúo en SI con alcance a toda la organización.
- El diseño e implementación de un programa de auditoria global de la SI.
- La implementación de todos los lineamientos de la norma ISO 27.001.

- Mejora Continua en SI: etapa de madurez que comprende los estadios "B" y "A" [2]. El objetivo aquí radica en el logro de la mejora continua en SI. Para ello, el Modelo de Madurez nos guiará en la implementación de varios requerimientos complejos, que no podrán ser alcanzados por cualquier tipo de organización.
  - **Estadio de Madurez "B":** se enfoca en mejorar significativamente la base implementada por el nivel anterior. Por este motivo, requiere de la utilización de métricas para evaluar y retroalimentar la gestión de seguridad, lo que configura un paso esencial en el logro de la mejora continua. A su vez, establece la necesidad de implementación de la norma de calidad ISO 9.001 y el establecimiento de un área organizativa responsable del diseño, implementación y mejora de procesos, como punto de partida para la gestión de la calidad de la SI [2]. A su vez, dicho nivel de madurez requiere de la implementación de las normas más importantes de la familia ISO 27.000[20], del estándar de continuidad

[20] Correspondientes a las normas ISO 27.001, 27.002, 27.003, 27.004, 27.005, 27.007 y 27.0014.

del negocio ISO 22.301 [21] y de unos de los componentes de gobierno de seguridad cruciales del MRU: el Comité Ejecutivo Permanente[21]. Constituye el gran salto desde una base común de Seguridad hacia la mejora continua. Este es el motivo por el cual el camino hacia la mejora continua en SI puede no ser adecuado para todas las organizaciones [2].

- **Estadio de Madurez "A":** se centra en el logro de la mejora continua en SI. Para ello requiere de la implementación de la metodología IAM de la NSA [23], cuyo principal eje se enfoca en el establecimiento de la conocida metodología del equipo rojo y equipo azul [22]. En dicho estadio se pretende implementar en forma completa los lineamientos de buenas prácticas del estándar del ISF [4] y de la sección del marco de trabajo COBIT [5] dirigida a la SI. Por último, requerirá de la implementación de un software BPMS (Sistema de Gestión de Procesos de Negocio) que ejecute la lógica de negocios de los procesos susceptibles de presentar aspectos o requerimientos de SI y, a su vez, de las medidas de Áreas de Extrema Seguridad[23] del MRU. Constituye el último estadio del Modelo de Madurez del MRU [2], enfocado en el logro de la mejora continua.

Los lineamientos comprendidos en cada estadio del Modelo de Madurez del MRU no han sido seleccionados en forma aleatoria, sino que responden a una cierta lógica que pretende traducir la Estrategia del MRU dentro del camino a recorrer desde el mínimo nivel de seguridad (estadio de madurez "F") hasta el máximo nivel de seguridad del MRU (estadio de madurez "A"). De esta forma, el Modelo de Madurez colabora con el trabajo de los profesionales de seguridad, estableciendo posibles caminos a seguir, priorizando los requerimientos a implementar, simplificando la comprensión de las buenas prácticas

[21] Favor de referirse al requerimiento LS1.2.10, incluido dentro del Trabajo Final de Especialización para mayor detalle sobre este organismo de gobierno de Seguridad de la Información.
[22] La práctica consiste en el establecimiento de dos equipos dentro de la organización: el rojo buscará, identificará y explotará vulnerabilidades de seguridad mientras que el azul se encargará de detectar la actividad del otro y detener su accionar.
[23] Consisten en medidas de seguridad no comunes y extremadamente excesivas y agresivas para la naturaleza del negocio de la gran mayoría de las organizaciones. Podrá encontrarse mayor detalle sobre estas medidas en el Anexo I del presente trabajo.

y agilizando la identificación de los requerimientos del MRU que mejor se adaptan a la naturaleza y a las necesidades de sus organizaciones.

Se incluye a continuación la nueva versión del Modelo de Madurez de SI (favor de referirse a la ilustración 2.3.2), en función de todos los lineamientos y mejoras detalladas anteriormente. El lector podrá fácilmente observar el nivel creciente en cuanto a complejidad de implementación y gestión de los requerimientos de SI vinculados a cada estadio de madurez. Cabe resaltar que, en función de lo detallado en el TFE, cada nivel requiere de la implementación de sus requerimientos específicos y de los requerimientos de todos los niveles inferiores a éste, para poder declarar conformidad con dicho estadio de madurez. Esto último ha sido modificado en cierta medida por el TFM, con el objetivo de flexibilizar la adaptabilidad del Modelo de Madurez de SI a cada organización, y a cada situación de implementación individual del Sistema de Mejora Continua en SI. Se procederá a describir con mayor detalle dichos cambios dentro de la sección 2.5 del presente trabajo.

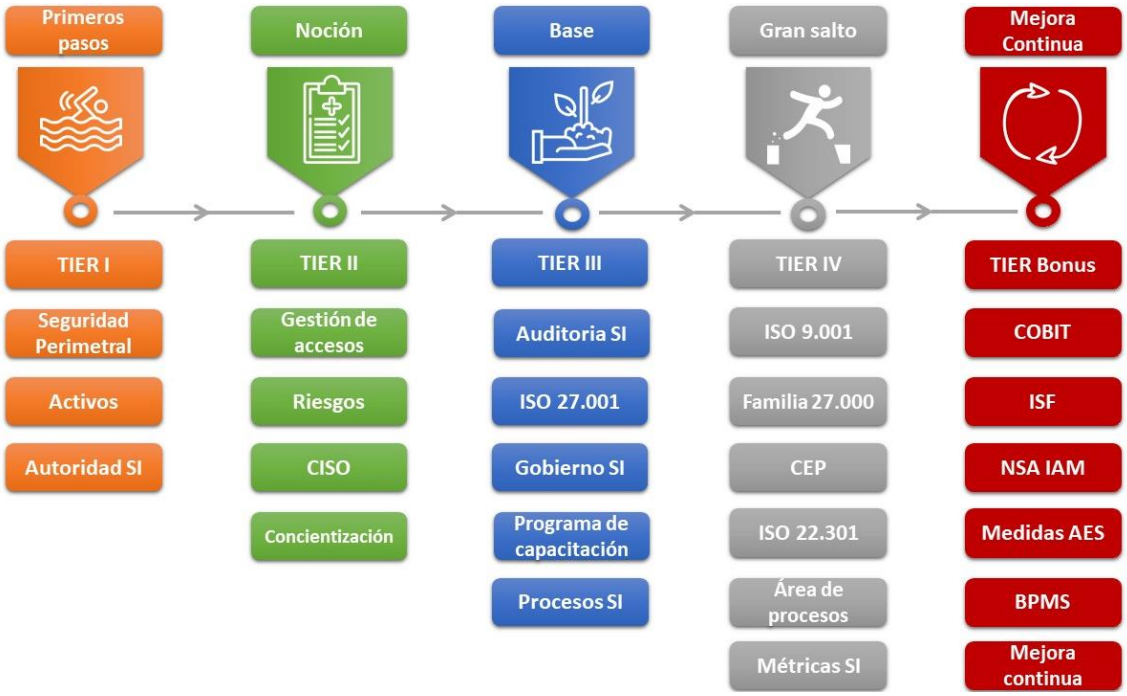

Ilustración 2.3.2: lineamientos individuales de cada estadio de madurez SI[24].

[24] CEP: Comité Ejecutivo Permanente (favor de referirse al requerimiento LS2.2.3 para conocer en detalle la función y propósito de este mecanismo de gobierno de SI implementado por el MRU).

Cabe aclarar que, el Modelo de Madurez ha sido diseñado teniendo en cuanta que el común de las organizaciones no llegará a implementar los máximos estadios de madurez, por lo que dichos niveles de madurez quedaran reservados exclusivamente para un pequeño y selecto grupo de organizaciones. Esto se debe a que los lineamientos de los niveles "A" y "B" además de ser significativamente complejos, variados y laboriosos de implementar, podrían llegar a ser incompatibles con ciertas organizaciones. Esta es la razón principal por lo que algunos lineamientos de seguridad no podrán ser alcanzados por cualquier tipo de organización. Todo dependerá efectivamente de la naturaleza de cada organización. Este es el motivo por el cual encontraremos a la gran mayoría de las organizaciones alineadas al estadio de madurez "C".

Se aconseja la búsqueda de los altos estadios de madurez únicamente para aquellas organizaciones que logren alinearse con las siguientes directivas:

- Tamaño de la organización: conforma el principal indicador sobre la posibilidad de que una organización logre alcanzar los estadios máximos de madurez. En primer lugar, cuanto más grande sea el tamaño de la organización, mayor será su necesidad de procurar acercarse al estadio de madurez "A". Por ejemplo, una organización pequeña bien podría conformarse con un estadio de madurez "D" y, a la vez, implementar un pequeño número de los requerimientos de niveles de madurez superiores que mejor se adapten a su naturaleza y objetivos estratégicos. Por lo tanto, no todas las organizaciones tendrán la necesidad, ni la voluntad, de afrontar el desafío de alcanzar los niveles de madurez máximos del MRU. Otro aspecto que debemos considerar consiste en la capacidad de las organizaciones para lidiar con la complejidad de los estadios de madurez superiores. Sin duda alguna, una organización multinacional de cientos de miles de empleados contará con mayores herramientas y, por ende, una significativa ventaja para enfrentar dicha complejidad que una pequeña o mediana organización de unos cuantos cientos de empleados. Es por este motivo, que el MRU recomienda que el estadio de madurez general objetivo para pequeñas organizaciones sea el nivel "D" y para organizaciones medianas el nivel "C". Para grandes

organizaciones, el MRU sugiere como mínimo el nivel intermedio “C+”, no obstante, recomendando la implementación para alcanzar en el mediano plazo el estadio de madurez “B”.

- Cultura de la organización: estipula otro indicador significativo que debe analizarse a la hora de seleccionar el nivel de madurez objetivo de la organización. Generalmente, la cultura de la organización nos brinda una clara perspectiva de la predisposición de sus recursos humanos a los altos estadios de madurez de seguridad. Si la cultura nos brinda una clara perspectiva de colaboración intra-organizacional, de la voluntad de afrontar nuevos desafíos (contando con una mínima o nula aversión al cambio y a la gestión de estos) y de seriedad de abordaje de proyectos de seguridad o similares, todo nos indica que la organización podrá alcanzar los estadios de madurez superiores. En cambio, si la cultura nos brinda una visión negativa de los aspectos discutidos anteriormente, sin lugar a dudas el proyecto de un Sistema de Mejora Continua vinculado a niveles de madurez iguales o superiores a “C” fracasará rotundamente.

- Naturaleza de la organización: conforma uno de los indicadores más significativos sobre la posibilidad de la organización de alcanzar estadios de madurez de seguridad superiores. Claramente, la naturaleza de la organización es un factor clave que influenciará la capacidad de la organización de alcanzar estos tipos de niveles de madurez, al encontrarse estrechamente vinculada a la seriedad con la que encarará las acciones de seguridad. Por ejemplo, si el modelo de negocio de la organización se basa fundamentalmente en el ahorro de costos, la capacidad de alcanzar los estadios de madurez “B” y “A” disminuye significativamente. Principalmente, debido a que estos niveles brindarán una gran dificultad a la hora de su implementación dentro de un presupuesto ajustado. A su vez, otro claro indicador radica en la existencia de algún mecanismo de gobierno corporativo dentro de la organización, ya que indicaría claramente que la organización podría encontrarse preparada para enfrentar la dificultad de los estadios superiores. La naturaleza de la organización nos indica fácilmente la capacidad de la organización de enfrentar seriamente las acciones de

seguridad requeridas por los estadios máximos de madurez y de generar valor en vez de destruirlos a través de las acciones de SI.

- Procesos de la organización: determina un claro indicador de la capacidad de la organización de luchar contra la complejidad. La adopción de la lógica de procesos de negocio conforma una metodología fundamental para simplificar y agilizar el trabajo de la organización con el objetivo de disminuir al máximo posible tanto la incertidumbre como la complejidad del camino a recorrer por los recursos humanos. Si la organización posee satisfactoriamente una cierta cantidad de procesos diseñados, implementados y mantenidos adecuadamente, su capacidad de afrontar altos niveles de madurez será adecuada. Cabe resaltar que la ejecución de los procesos de negocio conforma un requisito únicamente para el estadio máximo de madurez (correspondiente al nivel "A" del MRU).

- Base de SI de la organización: conforma otro significativo indicador de la capacidad de la organización para alcanzar estadios de madurez de seguridad superiores. Sin los controles generales de SI (tales como una correcta gestión de activos de información y una adecuada gestión de riesgos de SI) la organización jamás logrará alcanzar estadios de madurez superiores. Esto se debe a que los lineamientos de cada uno de los niveles de madurez se basan en la existencia de todos los lineamientos de los estadios inferiores. De esta forma, una organización jamás podrá alcanzar el nivel de madurez "C" si no cumple con las directivas de gestión de riesgos del nivel "D", ya que no podrá implementar varios de los requerimientos del nivel "C" que se basan en y requieren de la gestión de riegos de SI. Por lo tanto, sin las bases de seguridad no podremos movernos dentro del Modelo de Madurez. A su vez, si la organización no cuenta con los lineamientos de auditoria de la SI, del programa de capacitación de SI y los lineamientos de gobierno de seguridad, la concreción de los estadios superiores "B" y "A" conformaran una meta inalcanzable.

En conclusión, la decisión de una organización sobre la selección de un estadio de madurez objetivo conforma meramente una decisión de gestión de riesgos. Tomando en

consideración las cinco directivas detalladas anteriormente, las organizaciones deberán, en función de sus objetivos estratégicos, preguntarse: ¿Cuál es mi ubicación actual dentro del Modelo de Madurez?, ¿En qué posición dentro del Modelo de Madurez se encuentra la competencia?, ¿Qué nivel de madurez desearíamos tener? y ¿Qué estadio de madurez podríamos realmente llevar a la práctica en el mediano plazo? Estas preguntas son las que el macroproceso de implementación del Sistema de Mejora Continua colaborará en responder a las organizaciones que tomen la sabia decisión de implementar el MRU.

2.4 Capas de Seguridad de la Información

La presente sección pretende abordar en detalle el desarrollo de la Estrategia del MRU, uno de los objetivos a lograr por el presente TFM. Si bien la misma fue establecida durante la realización del TFE, se incorporará una visión más detallista de la Estrategia llevada adelante por el MRU, al profundizar tanto en sus características y componentes como en su estrecha interrelación con el Modelo de Madurez de SI.

La estrategia del MRU se encuentra conformada por siete componentes estratégicos, según lo detallado anteriormente dentro del TFE. No obstante, el presente trabajo modifica dicho esquema al reagrupar los componentes existentes, adicionar uno nuevo y modificar la estructura general por completo. De esta forma, se simplifica tanto el entendimiento de estrategia global del MRU como la visualización de la interrelación de esta con el Modelo de Madurez de SI. Por lo tanto, en función de las mejoras realizadas, la Estrategia del MRU se encontrará ahora conformada por cuatro componentes estratégicos, los cuales serán denominados como "*capas de SI*".

Las capas de SI conforman el plan estratégico sobre el cual se basa el MRU, ya que rigen y gobiernan todos los componentes de dicho marco de referencia. En otras palabras, componen la lógica existente detrás del MRU. Son aquellas que moldean el diseño y desarrollo tanto del Modelo de Madurez de SI como de la Colección de Buenas prácticas del MRU y cualquier otro de los componentes del Marco de Referencia Unificado en SI.

Las cuatro capas de SI del MRU se encuentran conformadas de la siguiente forma:

- Capa de Mejora Continua en SI: comprende la lógica detrás del Modelo de Madurez de SI. Se encuentra enfocado principalmente en la mejora a largo plazo de la SI de la organización a través del involucramiento de los Recursos Humanos a lo largo del diseño, implementación, mantenimiento y mejora del Sistema de Mejora Continua en SI que llevará adelante cada organización.

- Capa de Calidad de la SI: enfocada principalmente en la concreción de buenas prácticas en el área de seguridad, logra alcanzar su objetivo al combinar su implementación con la visión estratégica de la gestión orientada a procesos. A su vez, el presente componente estratégico es aquel que impulsa los mecanismos de gobierno de la SI del MRU.

- Capa de Controles Generales de Seguridad: comprende la base primordial de SI, que permitirá una implementación satisfactoria de los restantes componentes estratégicos. Se enfoca principalmente en la identificación y gestión de activos de información y su consecuente gestión de los riesgos de seguridad asociados a estos. De esta forma, se sientan las bases para la implementación de subsecuentes niveles de madurez, que de otra forma serian prácticamente inalcanzables sin una sólida base de SI.

- Capa de Enfoque en el Negocio: corresponde a la última capa del esquema estratégico del MRU. El propósito de este consiste en proveer una homogeneización entre los distintos componentes estratégicos del marco de referencia y, a la vez, establecer una dirección general estratégica unificada al priorizar el negocio, sus objetivos estratégicos y la creación de valor por parte de la organización.

Las cuatro capas de SI se encuentran firmemente entrelazadas entre sí, con el objetivo de establecer una dirección estratégica clara y concisa a la hora de diseñar e implementar un Sistema de Mejora Continua en SI.

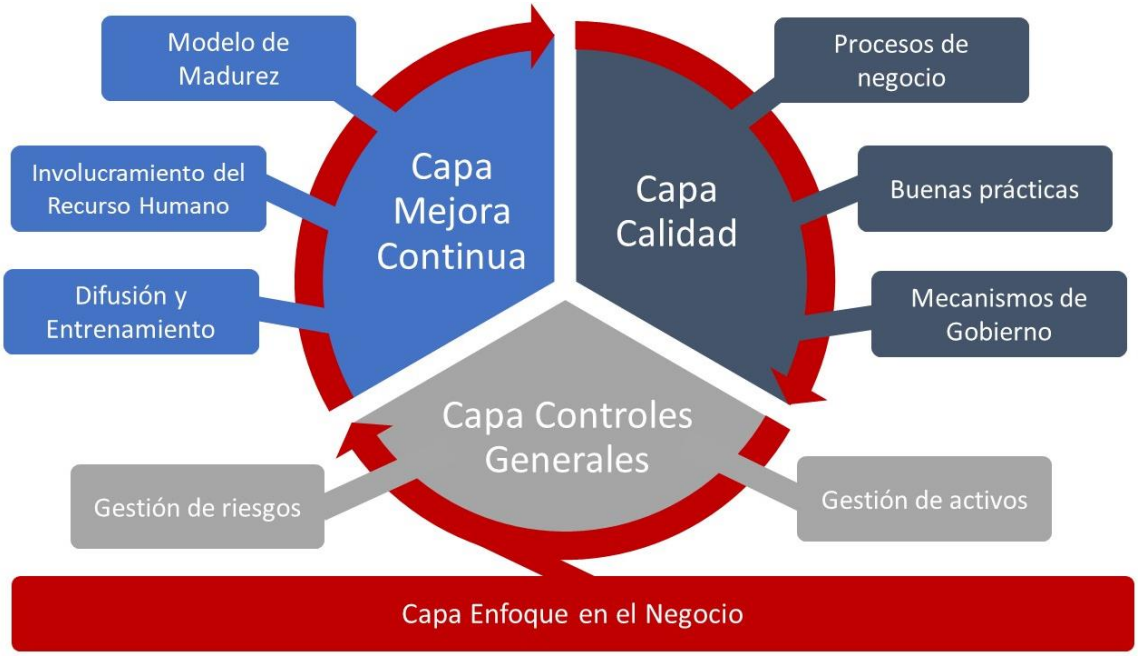

Ilustración 2.4.1: capas de SI del MRU.

Estos cuatro componentes estratégicos logran establecer una guía a seguir dentro del proceso de diseño y creación del MRU. De esta forma, se convierten en la lógica detrás de los componentes del marco de referencia, moldeando sus estructuras, gobernando sus respectivas implementaciones y entrelazándolos estrechamente entre sí. Pero ¿por qué es realmente necesaria la estrategia del MRU? Sin ella, no se podría lograr la integración entre sus distintos componentes, perdiendo así la coherencia entre los mismos. A su vez, sin la visión estratégica del MRU, la priorización de requerimientos de seguridad dentro del Modelo de Madurez conformaría una actividad meramente aleatoria y sin ningún basamento estratégico a seguir. Por último, la construcción de la colección de Mejores Prácticas carecería de sentido alguno, ya que las normas incorporadas serian seleccionadas al azar y sin tener en cuenta si realmente podrían llegar a brindar un beneficio a la organización y a la SI.

Pero ¿cómo lleva el MRU su estrategia a la práctica? Basándonos en la interrelación existente entre las capas de seguridad y el Modelo de Madurez, podremos visualizar el método establecido por el MRU. Pues, es el Sistema de Mejora Continua en SI el encargado en bajar a tierra y hacer realidad la estrategia del MRU. Este es el motivo por el cual las capas de seguridad gobiernan tanto la selección de las buenas prácticas como su clasificación dentro del Modelo de Madurez. De esta forma, toda organización que diseñe su propio Sistema de Mejora Continua en SI se encontrará consciente o inconscientemente siguiendo los pasos de la estrategia del MRU. El Sistema de Mejora Continua es aquel que lleva adelante los componentes estratégicos del Marco de Referencia Unificado en SI.

Las capas de SI actúan sobre el Modelo de Madurez de SI, gobernando los lineamientos requeridos para cada estadio de madurez. Son aquellas que establecen las guías sobre las cuales las organizaciones podrán moldear sus caminos a seguir. De esta forma, se convierten en los cimientos del MRU. Se incluye a continuación un diagrama que facilitará la visualización de la interrelación entre el Modelo de Madurez y las capas de SI (favor de referirse a la ilustración 2.4.2).

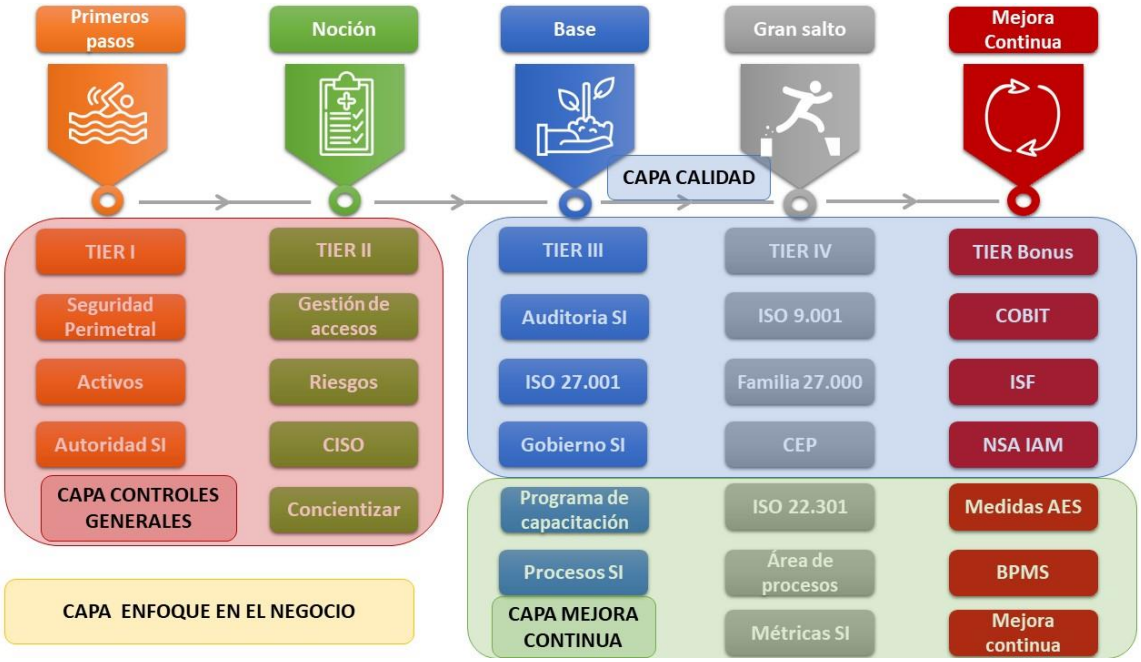

Ilustración 2.4.2: capas de Seguridad dentro del Modelo de Madurez.

Para finalizar, debemos hacer énfasis en que las Capas de SI conforman los cimientos del MRU, ya que son las que moldean no solo la estructura del marco de referencia sino también el diseño de cada uno de sus componentes.

2.5 Rigidez del Modelo de Madurez del MRU

Uno de los objetivos del presente TFM consistió en la adaptación del Modelo de Madurez de SI. La idea de dicha adaptación surgió de la puesta en común y discusión con colegas sobre los lineamientos fundamentales del MRU. De esta forma, se tomó conciencia de la rigidez que dicho modelo suponía para las organizaciones. Por ese motivo, el presente trabajo introduce ciertos cambios que colaboraran en la flexibilización de este:

- Flexibilización de los lineamientos obligatorios de cada estadio de madurez necesarios para manifestar la conformidad de una organización con un cierto nivel de madurez.
- Flexibilización de los lineamientos necesarios para manifestar la conformidad con un nivel intermedio de madurez de seguridad.
- El establecimiento del estadio general de madurez de las organizaciones.
- El diseño de los estadios individuales de madurez, por cada uno de los Subsistemas de SI del MRU.

El TFE estableció los diversos niveles de madurez del MRU, detallando que una organización podría únicamente asociarse a uno de estos niveles. El TFM modifica esta rigidez del modelo, estableciendo los estadios individuales de madurez. Por lo que, cada organización contará con nueve de estos niveles individuales de madurez por cada uno de los Subsistemas del MRU. De esta forma, los profesionales de seguridad podrán fácilmente conocer el estado actual de sus organizaciones y planificar ágilmente las acciones a llevar a cabo para mejorarlo. En función de estos nueve niveles individuales de madurez, surgirá el estadio general de madurez de la organización. En función de esto, la organización podrá generar un diagrama del tipo “araña” o radial con el objetivo de documentar y visualizar fácilmente sus estadios individuales de madurez de SI (esto último

es abordado en mayor detalle dentro de la sección 3.1 del presente trabajo). Se incluye a continuación un relevamiento de ejemplo sobre el estado actual de los niveles individuales de madurez de una organización hipotética, a los fines de detallar su propósito y utilidad. De dicho ejemplo podemos observar que la organización hipotética bajo análisis vincula cada uno de los estadios individuales de madurez con uno de los Subsistemas de SI del MRU.

Subsistema de Seguridad	Estadio Individual de Madurez
Gobierno de Seguridad	D
Lineamientos de Seguridad	A
Gestión de Riesgos	D
Ingeniería de Seguridad	E
Gestión de la Tecnología	D
Gestión de Recursos Humanos	B
Gestión de la Continuidad	C
Seguimiento y Control	C
Procesos y Mejora Continua	E

Estadios	F	E	D	C	B	A
Cantidad	0	2	3	2	1	1

Ilustración 2.5.1: relevamiento de ejemplo de los estadios de madurez individuales de una organización hipotética.

El presente relevamiento hipotético es un claro ejemplo de las diversas perspectivas y profundidades con las que una organización ataca las distintas áreas individuales de la SI. Es por este motivo, que el encasillamiento en un único estadio de madurez, tal como se estableció dentro del TFE, dificultaría el camino a recorrer por las

organizaciones, en vez de simplificarlo y agilizarlo acorde al objetivo fundamental del MRU. No obstante, la pregunta que debemos realizarnos ahora consiste en: ¿Cómo calcularemos el estadio general de madurez de una organización en función de sus niveles individuales de madurez? En otras palabras, ¿cómo lidiamos con tal disparidad de niveles de madurez? Para ello, necesitaremos establecer un mecanismo para el cálculo del estadio general de madurez de la organización en función de ciertos lineamientos que faciliten y flexibilicen la adaptación del Modelo de Madurez a cada situación específica de las organizaciones.

A primera vista, lo más sencillo a la hora de calcular el estadio general de madurez de una organización, consistiría en tomar el estadio individual de madurez más bajo con el cual manifiesta conformidad. No obstante, de esta forma estaríamos invalidando totalmente nuestro análisis sobre la organización, ya que el mismo se encontraría totalmente sesgado. Es por esta razón, que el presente trabajo introduce el concepto de "*saltos de madurez*". De esta forma, el Modelo de Madurez flexibiliza sus lineamientos para el cálculo del estadio general de madurez, con el objetivo de realizar un análisis holístico del estado de la SI de la organización.

Los saltos de madurez permiten alcanzar estadios generales de madurez mayores al menor estadio individual que posea la organización. Por ejemplo, la organización hipotética bajo análisis en la ilustración 2.5.1 poseería un nivel de madurez "E" según los lineamientos del TFE, no obstante gracias a las modificaciones realizadas al modelo, poseerá un nivel general de madurez "D". ¿Cómo se realiza el cálculo del estadio general de madurez de la organización? A través de los siguientes lineamientos:

- Un estadio individual de madurez "F" imposibilita el salto de madurez: de no cumplir con todos los requerimientos de nivel "E" de un cierto Subsistema de Seguridad, el estadio de madurez individual será calificado como "F". La existencia de niveles individuales "F" simboliza que la organización no se involucrado lo suficiente en el diseño de su Subsistema de Mejora Continua de SI. Por lo tanto, la organización que

posea al menos un estadio individual “F” no podrá realizar saltos de madurez para el cálculo de su estadio general de madurez.

- Imposibilidad de realizar saltos hacia los estadios generales de madurez “B” y “A”: dichos niveles de madurez simbolizan no solo el estado del arte en SI sino también la búsqueda de la mejora continua en la temática. Por lo tanto, no deberían existir atajos para alcanzar dichos estadios de madurez.

- Conformidad con todos los requerimientos clasificados como “claves” del estadio de madurez al que se pretende saltar dentro de todos los Subsistemas de Seguridad: el porcentaje de requerimientos claves del MRU es significativamente bajo, por lo que este lineamiento no agrega mayor dificultad a las implementaciones del marco de referencia. La organización deberá manifestar conformidad con todos los requerimientos claves del estadio de madurez objetivo, dentro de todos los Subsistemas de SI. De lo contrario, la organización podrá realizar un salto de madurez, pero hacia el estadio general de madurez intermedio inmediatamente inferior (siempre y cuando cumpla los lineamientos establecidos para los estadios de madurez intermedios). Por ejemplo, si nuestra organización hipotética (favor de referirse a la ilustración 2.5.1) no cumpliera con todos los requerimientos claves de nivel “D” de todos los Subsistemas de Seguridad, su nivel general de madurez podría encontrarse conformado por el nivel intermedio inmediatamente inferior “E+”, si es que manifiesta conformidad con todos los lineamientos para los niveles intermedios.

- Poseer una cantidad mayor de niveles individuales de madurez superiores del nivel al que se pretende realizar el salto que aquellos niveles inferiores al nivel objetivo a saltar: tomemos como ejemplo el caso de nuestra organización hipotética (favor de referirse a la ilustración 2.5.1), la cual desea saltar al nivel general “D”. Para ello debe calcular cuántos estadios individuales de madurez mayores al nivel “D” posee (efectivamente posee 4 niveles individuales superiores) y, a su vez, la cantidad de estadios individuales de madurez menores al nivel “D” que posee (efectivamente posee 2 niveles individuales inferiores). Como posee mayor cantidad de niveles superiores que

inferiores (4 niveles versus 2 niveles), su estadio general de madurez corresponde al nivel "D". De lo contrario, por ejemplo, si la organización pretendiera saltar al nivel general "C", no podría realizarlo. Esto se debe a que posee 5 estadios inferiores al nivel "C" (los niveles individuales "E" y "D" suman 5) en contraste con 2 estadios superiores al nivel "C" (los niveles individuales "A" y "B" suman 2).

La presente flexibilización del Modelo de Madurez de SI otorga una significativa ventaja durante las implementaciones, que será explotada efectivamente por el macroproceso de implementación del Sistema de Mejora Continua. El TFM abordará con mayor detalle esta temática durante el desarrollo del capítulo 3 del presente trabajo.

La flexibilización de los lineamientos de los estadios de madurez de seguridad alcanza, a su vez, a los estadios de madurez intermedios del MRU. Durante el TFE se han establecido 4 estadios de madurez intermedios (denominados "E+", "D+", "C+" y "B+"), cuyos lineamientos para manifestar conformidad eran los siguientes:

- Implementación del 20% de los requerimientos básicos[25] del estadio de madurez MRU inmediatamente superior.
- Implementación de todos los requerimientos clave[25] del estadio de madurez MRU inmediatamente superior.

El TFM mantiene la segunda condición y establece alternativas para reemplazar el cumplimiento de la primera. Por lo tanto, los lineamientos para los estadios intermedios de madurez se encontrarán conformados de la siguiente manera:

- Condiciones obligatorias:
  - Implementación de todos los requerimientos clave[15] del estadio de madurez MRU inmediatamente superior. Con la excepción para aquellas organizaciones que tengan la intención de realizar un salto de madurez, donde únicamente se

[25] El Modelo de Madurez clasifica los requerimientos del **MRU** en tres grandes grupos (básicos, claves y especiales), con el objetivo de identificar aquellos considerados importantes o complejos de implementar para así facilitar la concreción del estadio de madurez seleccionado por la organización. Podrá encontrarse mayor detalle sobre dicha clasificación en Anexo I del presente trabajo o en el TFE.

requerirá la implementación de los requerimientos clave del estadio de madurez inmediatamente inferior.

- No poseer ningún estadio individual de madurez de nivel “F”. Con la excepción para el estadio de madurez intermedio E+, la organización podrá poseer hasta 3 estadios individuales “F”.

- Manifestar conformidad con al menos una de las siguientes condiciones:

  - Implementación del 20% de los requerimientos básicos[25] del estadio de madurez MRU inmediatamente superior.
  - Poseer al menos tres estadios individuales de madurez de nivel “A”, únicamente valido para el estadio intermedio “B+”.
  - Poseer al menos dos estadios individuales de madurez de nivel “A”, únicamente valido para el estadio intermedio “C+”.
  - Poseer al menos un estadio individual de madurez de nivel “A”, únicamente valido para los estadios intermedios “E+” y “D+”.
  - Poseer al menos dos estadios individuales de madurez de nivel “B”, únicamente valido para los estadios intermedios “E+” y “D+”.
  - Poseer al menos tres estadios individuales de madurez de nivel “B”, únicamente valido para el estadio intermedio “C+”.
  - Poseer al menos tres estadios individuales de madurez de nivel “C”, únicamente valido para el estadio intermedio “D+”.
  - Poseer al menos dos estadios individuales de madurez de nivel “C”, únicamente valido para el estadio intermedio “E+”.

Los estadios individuales de madurez también podrán clasificarse utilizando estadios de madurez intermedios. No obstante, no son válidos como puntos extra a la hora de calcular el estadio general de madurez de la organización. Por lo tanto, un nivel individual de madurez “E+” se computa como un nivel individual “E”, un nivel individual de madurez “D+” se computa como un nivel individual “D” y así sucesivamente.

[Página dejada en blanco intencionalmente]

3

Macroproceso de implementación

El objetivo del presente capítulo del TFM consiste en dotar a los especialistas en seguridad de ciertos lineamientos que facilitarán significativamente una adopción exitosa del MRU dentro de cualquier tipo de organización. Dichos lineamientos estratégicos simplificaran el logro de los siguientes fundamentos esenciales requeridos para una correcta implementación del Sistema de Mejora Continua en SI:

- Visión organizacional única y unificada de la SI

  La adopción del MRU y la consecuente implementación del Sistema de Mejora Continua en SI no es algo que la organización debe tomarse a la ligera. Si la visión del futuro de la Seguridad no es homogénea dentro de la organización, el proyecto estará indefectiblemente condenado al fracaso. Una adhesión satisfactoria al MRU requiere de una visión única y unificada en cuanto a la SI de la organización desde arriba hacia abajo[26]. De lo contrario, las actividades de seguridad se limitarían únicamente a ciertos sectores de la organización, carecerán totalmente de apoyo por parte de la gestión y, a su vez, carecerían de una dirección estratégica global, resultando en acciones de seguridad dispares y arbitrarias con un alcance sesgado.

[26] Dicho enfoque hace referencia al establecimiento de una visión desde los altos estratos jerárquicos de la organización hacia los estratos jerárquicos inferiores.

- Voluntad de cambio

Desde el inicio del planeamiento de la adopción de la estrategia MRU, la organización deberá no solo manifestar la voluntad de cambio sino también reflejarla en sus acciones. Conforma uno de los lineamientos estratégicos fundamentales, debido a que el éxito de la implementación depende fundamentalmente del compromiso con el cambio tanto de la alta dirección como del órgano de gobierno de la organización. Lo cual deberá reflejarse en la asignación de recursos (materiales, humanos, tiempo, presupuesto, entre otros), en el establecimiento de un patrocinador de alto rango – preferentemente un representante del órgano de gobierno de la organización – para el proyecto global de adopción del MRU y en el establecimiento de una gestión del cambio integral a lo largo de todo el proyecto.

- Transmisión de valor

La transmisión de valor configura uno de los lineamientos estratégicos fundamentales de toda implementación de SI. Esto se debe a que, si no se transmite correctamente la visión del proyecto de adhesión al MRU a todos los estratos de la organización, el involucramiento y compromiso de los recursos humanos configurará un desafío imposible de lograr. En cambio, si la organización comunica adecuadamente el propósito tanto del cambio como del proyecto de seguridad, el personal de la organización le encontrará sentido a las acciones y procesos de gestión del cambio, disminuyendo significativamente la aversión al cambio.

- Involucramiento del Recurso Humano

En concordancia con el lineamiento estratégico anterior, los proyectos de seguridad fracasarán rotundamente si no se involucra al conjunto global de los recursos humanos de la organización desde su concepción inicial. Tanto sea para el planeamiento de acciones de seguridad como para las subsecuentes capacitaciones y acciones vinculadas a la gestión del cambio, el involucramiento del Recurso Humano conforma un requisito primordial de las implementaciones exitosas de SI.

Girando en torno a los lineamientos estratégicos - que conforman las directrices fundamentales para una implementación exitosa - detallados anteriormente, el presente capítulo se centrará en abordar en detalle la perspectiva de la implementación del MRU. Tanto el proceso de diseño como de implementación del Sistema de Mejora Continua en SI quedaban totalmente abiertos al criterio de los especialistas en seguridad. Es por este motivo, que el macroproceso de implementación establecerá claramente el camino a seguir, simplificando de esta forma las adopciones del MRU. Para lograr la definición de este camino a seguir, las organizaciones deberán, previo a la implementación y el diseño de su Sistema de Mejora Continua, encontrar una respuesta clara y unificada a las siguientes preguntas:

- ¿Cuál es mi ubicación actual dentro del Modelo de Madurez?
- ¿En qué posición dentro del Modelo de Madurez se encuentra la competencia?
- ¿Qué nivel de madurez desearíamos tener?
- ¿Qué estadio de madurez podríamos realmente llevar a la práctica?

Estas preguntas son las que el macroproceso de implementación del Sistema de Mejora Continua tomará como input necesario para su ejecución. Y es así como guiará a las organizaciones a través de la complejidad para alcanzar los estadios de madurez de seguridad acordes tanto a su naturaleza como a sus objetivos estratégicos.

3.1 Análisis de madurez de SI

Previo al diseño de su propio Subsistema de Mejora Continua, cada organización deberá realizar un análisis de madurez de su SI. El objetivo de dicho análisis radica en encontrar las respuestas a ciertos interrogantes estratégicos, que definirán los lineamientos base que los profesionales de seguridad deberán tener en cuenta a la hora de diseñar los Sistemas de Mejora Continua. De esta forma, los profesionales se asegurarán de que sus diseños se encuentren acordes tanto a la visión de la organización como a sus objetivos estratégicos. En cierta forma, el análisis de madurez que establece

el presente trabajo permite alinear la estrategia corporativa de la organización tanto a su estrategia de SI como a la estrategia del MRU, permitiendo así que las acciones de seguridad generen valor en lugar de obstaculizar su creación o, peor aún, destruirlo.

El análisis de madurez consistirá en el descubrimiento de 4 estadios de SI. Dichos estadios medirán diversas variables estratégicas, sentando así las bases del camino a recorrer a través del Modelo de Madurez de SI. Pues, al lograr identificar los 4 estadios de Seguridad la organización podrá contar con un claro panorama para definir su estrategia de SI y, por ende, sus pasos a seguir a través del Modelo de Madurez del MRU. Los estadios de madurez de SI se encuentran configurados de la siguiente forma:

1. Situación actual de la organización, dentro del Modelo de Madurez del MRU

   La organización deberá encontrar una respuesta a la siguiente pregunta estratégica: ¿Cuál es mi ubicación actual dentro del Modelo de Madurez? El objetivo aquí es establecer el nivel general madurez de la organización, en otras palabras, definir el estado AS-IS en función de los lineamientos de madurez del MRU. De esta forma, la organización comenzará a tener un panorama más claro, ya que si no conoce su situación actual le será imposible estimar las medidas y acciones necesarias para alcanzar un estadio de madurez superior deseado.

2. Situación futura deseada de la organización, dentro del Modelo de Madurez

   Aquí la organización deberá encontrar un nivel general de madurez objetivo que se encuentre alineado a sus objetivos estratégicos. El presente estado de SI configura una expresión de deseo de la organización, al no tomar en consideración principalmente los recursos necesarios y muchas otras variables que entrarían en juego si se buscase una situación futura factible.

   La organización deberá encontrar una respuesta a la siguiente pregunta estratégica: ¿Qué nivel de madurez desearíamos tener (situación deseada)? La clave aquí consiste en encontrar un estadio general de madurez alineado a su naturaleza. Dejando de lado otras variables (tales como el compromiso de los RRHH o la disponibilidad de recursos), la organización deberá enfocarse en identificar el estadio

de madurez más alto al que esperaría alcanzar en el largo plazo, siempre que este se adecue a su naturaleza. Por ejemplo, de nada serviría que una pequeña organización de nivel general "E" establezca como nivel futuro deseado el estadio de madurez "B", ya que sencillamente tal elevado nivel de madurez no se alineará jamás a su naturaleza - su estructura, su estrategia corporativa, su cultura. No obstante, podría si conformar su situación deseada en el estadio general de madurez "C", el cual en el largo plazo podría alinearse a su naturaleza.

3. Situación futura factible de la organización, dentro del Modelo de Madurez

Aquí la organización deberá encontrar un nivel general de madurez factible que pueda alinearse tanto a sus recursos como a su naturaleza y a su voluntad de cambio. La identificación de este estadio de SI deberá basarse en un estadio general de madurez factible de implementar en el mediano plazo por la organización. Si retomamos al ejemplo detallado en el apartado anterior, de nada serviría que la pequeña organización de nivel general "E" y estadio de seguridad deseado "C", establezca como nivel futuro factible el estadio de madurez "C" o "D+", ya que jamás logrará contar con los recursos necesarios para lograrlo en el mediano plazo. A su vez, difícilmente logre hacer realidad su voluntad de cambio ante tan significativas alteraciones a su normal funcionamiento, y sin siquiera analizar si efectivamente tal transformación debe necesariamente implementarse en forma tan apresurada.

La organización deberá encontrar una respuesta ponderada a las siguientes preguntas estratégicas: ¿Qué nivel de madurez desearíamos tener (situación deseada)? y ¿Qué estadio de madurez podríamos realmente llevar a la práctica (situación deseada factible)? La clave aquí consiste en encontrar un estadio general de madurez factible de implementar por la organización y, a la vez, alineado a su naturaleza. Los especialistas de seguridad podrían realizar un promedio entre las respuestas a estas preguntas o bien establecer un promedio ponderado basado en las necesidades y posibilidades de la organización. La decisión quedará a criterio de los especialistas en seguridad.

4. Posición actual de la competencia, dentro del Modelo de Madurez

La organización deberá encontrar una respuesta a la siguiente pregunta estratégica: ¿En qué posición dentro del Modelo de Madurez se encuentra nuestra competencia? La confección de esta respuesta configura la más compleja de los 4 estadios de seguridad. Esto se debe a la extensa variación de la naturaleza de la competencia entre diversos sectores del mercado. Cada organización individual enfrentará un sin número de posibilidades de escenarios diferentes de competencia. El escenario más sencillo que una organización podría poseer, por ejemplo, se encontraría conformado por un único competidor, en donde fácilmente obtendríamos la respuesta buscada. En cambio, si nos enfrentamos a un significativo número de jugadores en el mercado: ¿tomaremos un promedio o una media del estado general de madurez de la industria? o ¿tomaríamos el máximo de la industria a modo de inspiración o el mínimo para simplificar nuestro trabajo? Es por este motivo, que la respuesta será claramente subjetiva basada en el criterio de cada especialista de seguridad y, fundamentalmente, en la naturaleza del negocio de la organización.

Una vez obtenidos los 4 estadios de SI, cada organización contará con un claro panorama de cómo encarar su implementación individual del MRU. De esta forma, logrará obtener el input clave necesario para una satisfactoria ejecución del macroproceso de implementación. Se incluye a continuación la definición de los 4 estadios de SI de una organización hipotética, los cuales pueden visualizarse dentro de la ilustración 3.1.1.

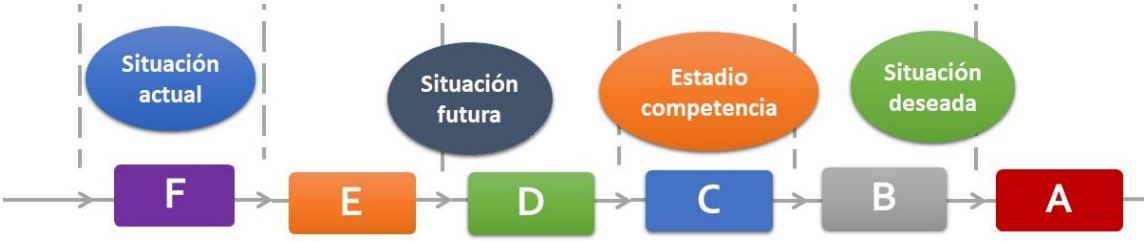

Ilustración 3.1.1: relevamiento de ejemplo de los estadios de SI de una organización hipotética.

El MRU recomienda que el análisis de madurez produzca como resultado un diagrama del tipo radial - mejor conocido como gráfico "*araña*" - reflejando los 4 estadios de SI en función de los niveles individuales de madurez de la organización. De esta forma, el especialista en seguridad poseerá el desarrollo completo de la situación actual de SI sobre la que deberá accionar. De aquí surgen los primeros pasos de la implementación del Sistema de Mejora Continua, al definirse los lineamientos de:

- La identificación de las buenas prácticas del MRU que mejor se alinean a la naturaleza de la organización. Con el objetivo de priorizar la adhesión únicamente de aquellos requerimientos de seguridad que mejor combinen con la organización y sus objetivos estratégicos. De esta forma los especialistas en seguridad simplificarán la complejidad de la identificación, selección y posterior implementación de las buenas prácticas de seguridad del MRU.
- El diseño e implementación del Sistema de Mejora Continua de la organización por primera vez. En función de las buenas prácticas identificadas anteriormente, los especialistas en seguridad construirán dicho sistema que le permitirá a la organización el logro de su estadio de madurez objetivo.
- El diseño e implementación de mejoras al Sistema de Mejora Continua de la organización con el objetivo de realizar saltos de madurez. Identificando las buenas prácticas necesarias a implementar y los ajustes necesarios al Sistema de Mejora Continua de la organización para cumplir con los requisitos necesarios para lograr el salto de madurez.

¿Cómo es que logramos construir el diagrama araña de la situación de seguridad de nuestra organización? Con el objetivo de facilitar dicha tarea, el macroproceso de implementación ha sido dotado de un mecanismo genérico de relevamiento y documentación de los estadios en función de los niveles individuales de madurez respectivos. En primer lugar, se deberán establecer el nivel individual de madurez de la organización por cada uno de los Subsistemas de Seguridad del MRU (representado en la

ilustración 3.1.2 por el segmento azul "*As Is*[27]"). El segundo paso consistirá en el establecimiento del nivel "*benchmark*[28]" - estadio de madurez indicativo de la competencia directa de la organización - representado por el segmento de color gris en la ilustración 3.1.2. Por último, se procederá a establecer los niveles individuales de madurez objetivo (aquellos niveles factibles de implementarse en el mediano plazo) de la organización, representados por el segmento de color rojo "*To be*[29]" en la ilustración 3.1.2. Con estos tres segmentos establecidos, se configura el producto final del proceso de análisis de madurez de la SI de una organización - el cual corresponde al primer paso del macroproceso de implantación del Sistema de Mejora Continua del MRU.

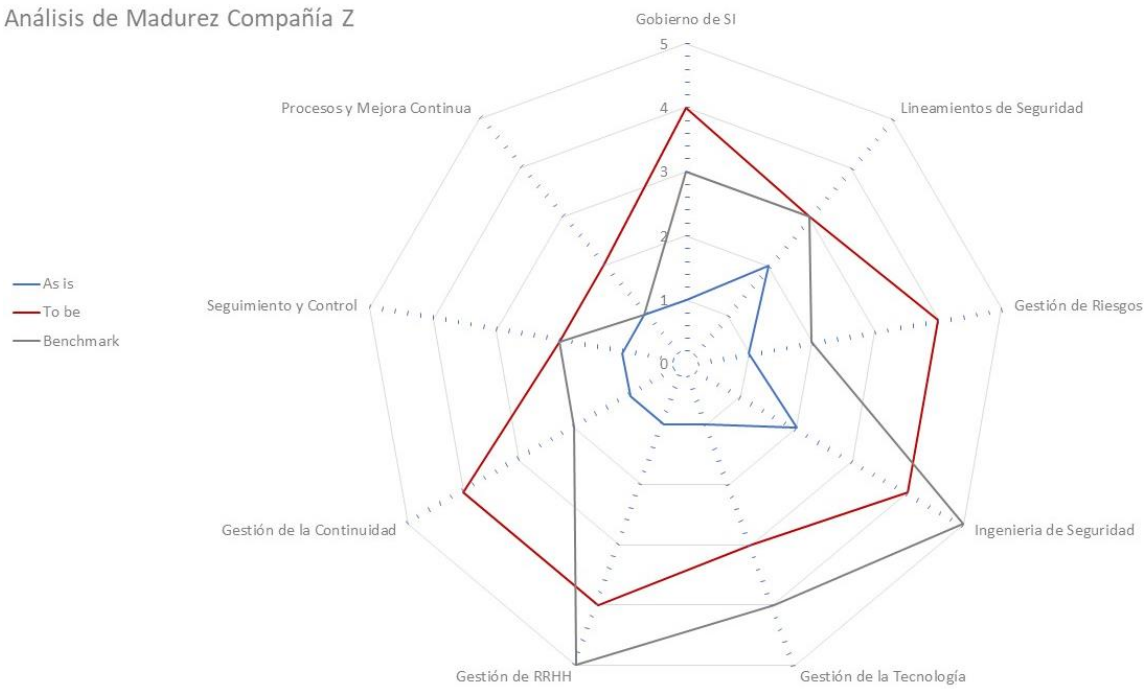

Ilustración 3.1.2: diagrama "araña" de los estadios Seguridad de una organización hipotética, en función de sus niveles individuales de madurez.

[27] Hace referencia al estado actual de la organización - así tal como se encuentra actualmente - en una cierta temática (en este caso la Seguridad de la Información).
[28] Hace referencia al estado actual de la competencia de la organización en una cierta temática, en este caso la Seguridad de la Información.
[29] Hace referencia al estado futuro de la organización en una cierta temática (en este caso la Seguridad de la Información).

El diagrama incluido dentro de la ilustración 3.1.2 conforma el producto final del análisis de madurez de SI. Los semielaborados o productos intermedios de dicho proceso conforman las siguientes matrices de implementación:

- Matriz de estadios individuales de madurez actuales de la organización. Estableciendo el nivel individual de madurez de la organización por cada uno de los Subsistemas de SI. Podrá observarse un ejemplo de esta matriz dentro de la ilustración 3.1.3, donde se establecen 3 variables: estadio individual de madurez de cada subsistema, la ponderación de dichos estadios individuales (con el objetivo de aproximar los estadios intermedios al nivel inmediato inferior) y el estadio numérico (el cual convierte a cada estadio de madurez en su versión numérica, donde 1 representa el nivel mínimo de madurez "E" y 5 representa el nivel máximo de madurez "A"). El objetivo de la presente matriz consiste en marcar el grado de cumplimiento de la organización con los lineamientos de madurez de cada uno de los subsistemas de SI del MRU.

MRU	Matriz As Is		
	Estadio individual	Ponderación	Estadio numérico
Gobierno de SI	E	E	1
Lineamientos de Seguridad	D	D	2
Gestión de Riesgos	E	E	1
Ingenieria de Seguridad	D+	D	2
Gestión de la Tecnología	E	E	1
Gestión de RRHH	E+	E	1
Gestión de la Continuidad	E	E	1
Seguimiento y Control	E+	E	1
Procesos y Mejora Continua	E	E	1

Ilustración 3.1.3: matriz de estadios individuales de madurez actuales de una organización hipotética.

- Matriz de estadios individuales de madurez actuales de la competencia. Establece el nivel individual de madurez de la competencia por cada uno de los Subsistemas de SI. Podrá observarse un ejemplo de dicha matriz dentro de la ilustración 3.1.4, donde se establecen las mismas 3 variables detalladas en la matriz analizada anteriormente: estadio individual de madurez de cada subsistema, la ponderación de dichos estadios individuales y el estadio numérico (el cual convierte a cada estadio de madurez en su versión numérica, utilizando la misma mecánica detallada en el apartado anterior). El objetivo de esta consiste en visualizar el grado de avance en seguridad de la competencia, en función los lineamientos de madurez de cada uno de los subsistemas de SI del MRU.

MRU	Matriz Benchmark		
	Estadio individual	Ponderación	Estadio numérico
Gobierno de SI	C	C	3
Lineamientos de Seguridad	C	C	3
Gestión de Riesgos	D	D	2
Ingenieria de Seguridad	A	A	5
Gestión de la Tecnología	B	B	4
Gestión de RRHH	A	A	5
Gestión de la Continuidad	D	D	2
Seguimiento y Control	D	D	2
Procesos y Mejora Continua	E	E	1

Ilustración 3.1.4: matriz de estadios de madurez benchmark de una organización hipotética.

- Matriz de estadios individuales de madurez objetivos de la organización. Establece el nivel individual de madurez objetivo de la organización por cada uno de los Subsistemas de SI. Podrá observarse un ejemplo de esta dentro de la ilustración 3.1.5, donde se establecen las mismas 3 variables detalladas en las matrices anteriores. El objetivo de la presente matriz consiste en establecer estadios individuales de madurez factibles de alcanzar por la organización en el mediano plazo. Dichos

estadios surgirán de la ponderación de la situación futura deseada y la situación futura factible de madurez de la organización, en función los lineamientos de madurez de cada uno de los subsistemas de SI del MRU.

MRU	Matriz To Be		
	Estadio individual	Ponderación	Estadio numérico
Gobierno de SI	B+	B	4
Lineamientos de Seguridad	A	A	5
Gestión de Riesgos	B	B	4
Ingenieria de Seguridad	B	B	4
Gestión de la Tecnología	C+	C	3
Gestión de RRHH	B	B	4
Gestión de la Continuidad	B	B	4
Seguimiento y Control	D+	D	2
Procesos y Mejora Continua	D	D	2

Ilustración 3.1.5: matriz de estadios individuales de madurez objetivos de una organización hipotética.

3.2 Mapa de macroprocesos de implementación del MRU

El macroproceso de implementación del MRU se encuentra conformado por una serie de Macroprocesos de menor nivel. Los cuales, en conjunto, establecen la lógica a seguir por parte del macroproceso. Son, en un cierto sentido, las partes que lo conforman y que establecen la dirección estratégica de todas las actividades y procesos de implementación del MRU. Debido a que estos componentes se encuentran estrechamente interrelacionados a través de una lógica única predeterminada, las buenas prácticas dictan la construcción de un mapa de macroprocesos para el logro de su efectivo análisis y gestión.

La presente sección del trabajo se enfocará en establecer el mapa de macroprocesos de implementación guía del MRU. Se procederá al detalle global de los mismos y sus interrelaciones, finalizando con una breve descripción individual de cada

uno de ellos. Los macroprocesos se encuentran dividíos en función de la metodología "*Plan, Do, Check, Act*"[30] [1] establecida por las normas ISO.

Se incluye a continuación, dentro de la ilustración 3.2.1, el esquema fundamental del macroproceso de implementación del Sistema de Mejora Continua en SI.

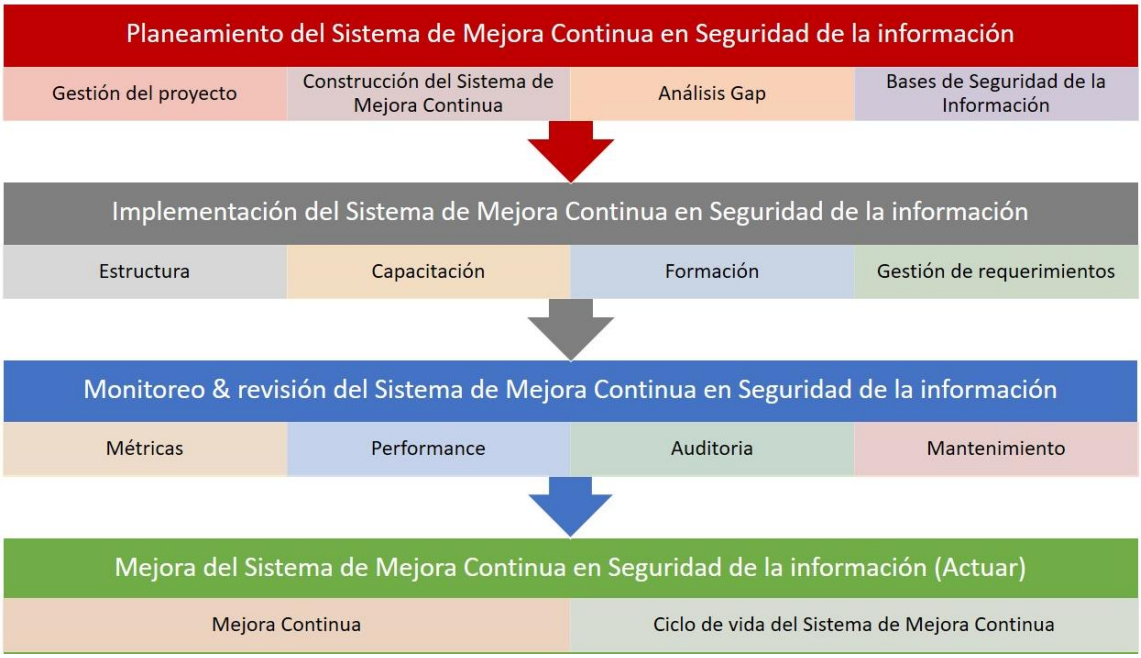

Ilustración 3.2.1: macroproceso de implementación del Sistema de Mejora Continua en Seguridad de la Información.

[30] En su traducción al español: Planear, hacer o implementar, monitorear o revisar y actuar.

Etapa 1: planeamiento

El objetivo de esta etapa consiste principalmente en el relevamiento de las necesidades de la organización y en el diseño del Sistema de Mejora Continua de la organización en función de sus necesidades relevadas. Para ello recurrirá a múltiples macroprocesos enfocados tanto en la estructuración del marco de referencia de gestión estratégica de la SI (Gobierno, estructura, autoridades, políticas y procesos de seguridad) como en la ejecución de actividades base de seguridad (gestión de los activos de información y la evaluación de sus correspondientes riesgos de SI). A continuación, podrá observarse dentro de la ilustración 3.2.2, los macroprocesos que componen esta primera etapa de planeamiento del Sistema de Mejora Continua en SI.

Ilustración 3.2.2: macroprocesos pertenecientes a la etapa 1 (planeamiento).

1. *Gestión del plan de proyecto*

Ilustración 3.2.2: macroprocesos de nivel 2 que componen el macroproceso de nivel 1: Gestión del plan de proyecto

Objetivos

- "*Comprender las necesidades de la organización*" [19].
- Comprender la naturaleza (su estructura, su cultura, su forma de realizar su negocio) y su situación actual relativa a la SI de la organización.
- Entender la forma de trabajo de la organización (sus mecanismos de gobierno y de definición de políticas y procesos).
- Comprender como se alinean los apartados anteriores con los objetivos estratégicos corporativos para así poder definir en forma alineada los objetivos estratégicos de SI de la organización.
- Relevar la situación actual de la competencia relativa a la SI, a los fines de aclarar el panorama estratégico de seguridad de la organización.
- Conformar el estado futuro objetivo de la organización relativo a la SI.

- Asegurarse que la dirección ejecutiva y el órgano rector de gobierno de la organización "*comprendan el caso de negocio de una implementación del*" [20] MRU, al expresar su "*aprobación del plan de proyecto*" [20] y su "*compromiso de implementación de un*" [20] Sistema de Mejora Continua en SI.

Descripción

Macroproceso inicial de implementación del MRU. Conforma los primeros pasos a seguir durante la identificación de las necesidades de la organización, el establecimiento de sus prioridades, la definición del alcance, los actores involucrados, el contexto, y la identificación de los requerimientos a cumplir. Requiere la aprobación de la alta dirección y, de existir, del órgano de gobierno corporativo de la organización. Uno de sus objetivos fundamentales se basa en "*demostrar y establecer el valor de la SI a la organización*" [20] y, a su vez, se enfoca en establecer los 4 estadios de SI (establecidos en la sección 3.1 del presente trabajo).

Entradas ("Inputs")

- "*Objetivos estratégicos de la organización*" [20].
- Análisis de la "*visión general de los sistemas de gestión actuales de la organización*" [20], incluyendo aquellos que se encuentren en etapa de estudio y/o construcción.
- "*Requerimientos legales, regulatorios, contractuales,*" [20] estatutarios y de mercado "*vinculados y/o aplicables a la organización*" [20].

Macroprocesos principales

- Gestión del Contexto de la organización.
    - "*Identificación de las prioridades y necesidades de la organización*" [20].
    - "*Identificación de los objetivos estratégicos de la organización*" [20].
    - "*Identificación de los requerimientos legales, regulatorios, contractuales*" [20], estatutarios y de mercado "*vinculados y/o aplicables a la organización*" [20].
    - "*Identificación de las características (naturaleza) del negocio*" [20].

- "*Establecimiento del alcance del*" [20] Sistema de Mejora Continua de la organización, en función de LS1.1.4

- Análisis de Madurez de SI (para mayor detalle de este macroproceso, favor de referirse a la sección 3.1 del presente trabajo).
- Generación y aprobación del plan de proyecto.
  - "*Construcción del caso de negocio*" [20] de adhesión al MRU.
  - "*Definición preliminar de autoridades, responsabilidades*" [20] y facultades.
  - "*Diseño de la propuesta de plan de proyecto*" [20].
  - "*Aprobación del plan de proyecto*" [20].

Salidas ("Outputs")

- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- "*Documentación de los requerimientos legales, regulatorios, contractuales,*" [20] estatutarios y de mercado "*vinculados y/o aplicables a la organización*" [20].
- "*Documentación de las características salientes del negocio, de la organización, de sus ubicaciones, activos y tecnología*" [20].
- "*Documentación del alcance del proyecto*" [20].
- Caso de negocio de adhesión al MRU e implementación de un Sistema de Mejora Continua en SI. El caso establecerá:
  - "*Las prioridades y los objetivos de la implementación del*" [20] Sistema de Mejora Continua.
  - El marco de referencia preliminar[31] de gobierno de SI de la organización.
  - La estructura ejecutiva preliminar[32] de gestión de la SI de la organización (roles, responsabilidades y facultades) [20].

[31] Dentro del plan de proyecto se establecerán únicamente los lineamientos principales. Luego en etapas más avanzadas se definirá en forma detallada y completa el mecanismo de gobierno de Seguridad de la información que utilizará la organización.
[32] Dentro del plan de proyecto se establecerán únicamente los lineamientos principales. Luego en etapas más avanzadas se definirá en forma detallada y completa el mecanismo de gobierno de Seguridad de la información que utilizará la organización.

- Acta de aprobación del proyecto de adhesión al MRU.
- Acta compromiso de implementación del Sistema de Mejora Continua en SI (comprometiendo la asignación de recursos, tiempos, prioridades y un patrocinador al proyecto). El acta documentará el "*compromiso de asignación de recursos durante el diseño e implementación del proyecto*" [20].
- "*Plan de proyecto que indique los distintos hitos (tales como la gestión de riesgos, la implementación del*" [20] Sistema de Mejora Continua en SI*, "la realización de auditorías y la revisión gerencial)*" [20].

2. *Construcción preliminar del Sistema de Mejora Continua*

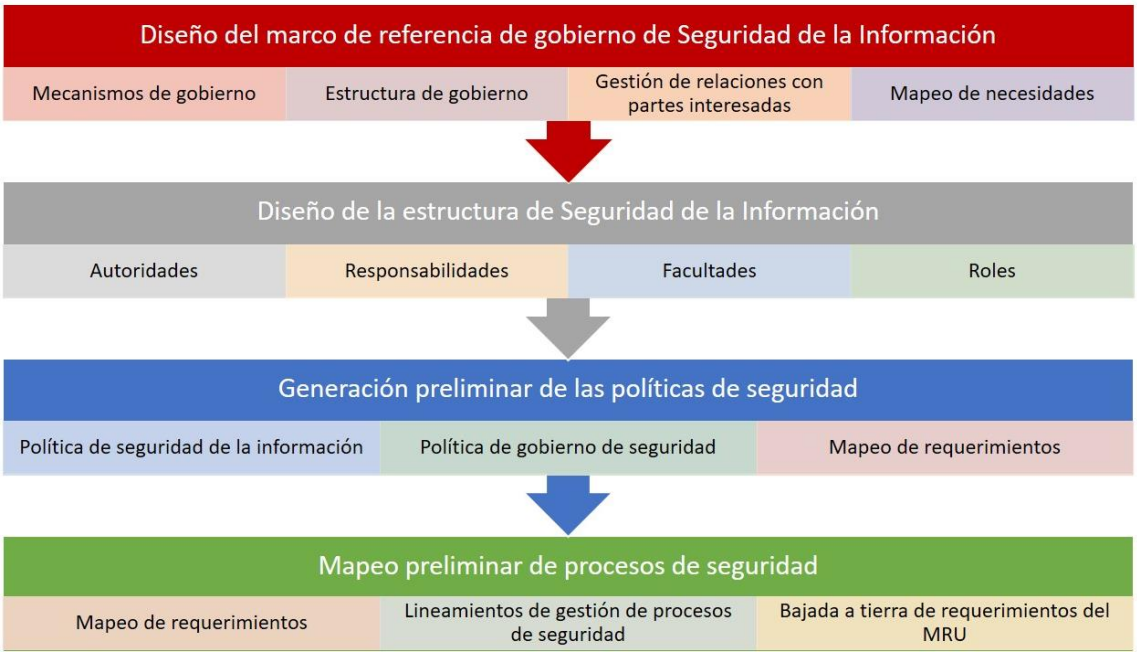

Ilustración 3.2.3: macroprocesos de nivel 2 que componen el macroproceso de nivel 1: Construcción preliminar del Sistema de Mejora Continua

Objetivos

- Desarrollo de la política de SI.
- Desarrollo de la política de gobierno de SI.
- Diseño de mecanismos de gobierno de SI.

- Aprobación del marco de referencia de gobierno de SI por parte del órgano rector de gobierno de la organización.
- Diseño definitivo de la estructura de SI de la organización.
- Establecimiento de los roles, autoridades, responsabilidades y facultades definitivas de SI de la organización.
- Mapeo de las necesidades de la organización en relación a la SI.
- Gestión de la relación con las partes interesadas en materia de SI.
- Mapeo preliminar de procesos de seguridad, bajando a tierra lo establecido en los Subsistemas GOB (Gobierno de SI) y LS (Lineamientos de SI) del MRU.

Descripción

Siendo el segundo macroproceso de implementación del MRU, el mismo se enfocará en dar detalle tanto al mecanismo de gobierno de seguridad como a la estructura de SI (establecidas en forma preliminar en el macroproceso anterior). El objetivo consiste en enfocarse primordialmente en el mapeo de los requerimientos de los Subsistemas (Gobierno de SI) y LS (Lineamientos de SI) del MRU, para subsecuentemente establecer las políticas primordiales de dichos Subsistemas (la política de SI y la política de gobierno de SI) para su correspondiente bajada a tierra a procesos. Hasta este punto, la organización solo requerirá tener claramente definidos que estadios de madurez querrá implementar únicamente para los dos Subsistemas bajo a análisis por el presente macroproceso.

Entradas ("Inputs")

- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- Estadios de SI.
- Estructura preliminar de seguridad.
- Caso de negocio aprobado por el órgano rector de gobierno de la organización.

Macroprocesos principales

- Diseño del marco de referencia de gobierno de SI.
  - Diseño y documentación de los mecanismos de gobierno de seguridad.
  - Conformación de la estructura y organismos de gobierno de seguridad.
  - Gestión de relaciones con partes interesadas vinculadas a la SI.
  - Mapeo de necesidades de la organización con los requerimientos pertinentes del MRU.
- Diseño de la estructura de SI.
  - Desarrollo de las autoridades de SI, en función de LS2.2.
  - Establecimiento de las responsabilidades, roles y facultades de las autoridades de SI.
  - Aprobación de la estructura por parte de la dirección ejecutiva de la organización.
- Generación preliminar de las políticas de seguridad.
  - Mapeo de requerimientos de los estadios individuales de madurez objetivos correspondientes a los subsistemas LS y GOB.
  - Diseño, aprobación e implementación de la política de SI.
  - Diseño, aprobación e implementación de la política de gobierno de SI.
- Mapeo preliminar de procesos de seguridad.
  - Desarrollo del mapeo de requerimientos de bajo y alto nivel (bajada a tierra de los requerimientos del MRU).
  - Diseño e implementación de los lineamientos de gestión de procesos de seguridad (de alto y bajo nivel).

Salidas (“Outputs”)

- “*Matriz RACI preliminar, conteniendo todos los roles, responsabilidades y facultades de las autoridades de SI*” [20].
- “*Procesos preliminares sobre la jerarquía de decisiones de seguridad y, a su vez, sobre la estructura del*” [20] Sistema de Mejora Continua en SI.

- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.
- Documentación de roles y autoridades de SI.
- Mapeo preliminar de requerimientos del MRU.

3. *Gestión de activos de información*

Objetivos

- "*Identificar a los activos de información de la organización, que serán soportados por el*" [20] Sistema de Mejora Continua en SI.
- Clasificar los activos de información de la organización en función de los lineamientos establecidos en LS2.3 que se alineen al nivel de madurez objetivo de la organización.

Descripción

El presente macroproceso se enfoca en la creación del inventario de activos de información de la organización, con el objetivo de dar el puntapié inicial para la subsecuente gestión de riesgos. Si no tenemos en claro cuáles son nuestros activos, no podremos realizar una buena gestión de riesgos. A su vez, se establecerá el valor de los activos de información y se los clasificará en función de los lineamientos del MRU y las disposiciones específicas de cada organización.

Entradas ("Inputs")

- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- Estadios de SI.
- Estructura preliminar de seguridad.

- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.
- Documentación de roles y autoridades de SI
- Mapeo preliminar de requerimientos del MRU.
- "*Requerimientos de SI*" [20] identificados anteriormente dentro del primer macroproceso de implementación.

Macroprocesos principales

La definición, estructura y mecanismos del presente macroproceso quedan supeditados al libre criterio de la organización, siempre y cuando cumpla con los requerimientos del MRU vinculados a su estadio de madurez objetivo.

Salidas ("Outputs")

- Inventario de activos de información de la organización (en función del alcance establecido para el proyecto).
- Documentación de "*la clasificación de los activos de información de la organización*" [20].
- Clasificación de los Activos de información de la organización según su criticidad, en función de los lineamientos establecidos por el requerimiento LS2.3.6.

4. *Gestión de riesgos de SI*

Objetivos

- "*Definir y establecer la metodología de gestión de riesgos de SI*" [20].
- "*Evaluar los riesgos relativos a la SI de la organización*" [19].
- "*Identificar, analizar y tratar los riesgos de SI*" [20].
- Disminuir el nivel residual de los riesgos de SI hasta un nivel aceptable, en función del apetito de riesgos definido por el órgano rector de gobierno de la organización.

- Establecimiento y documentación del apetito de riesgos de la organización.

Descripción

El presente macroproceso gira en torno a la primera gestión de riesgos de SI que la organización ejecutará (siempre y cuando configure una organización con su primera implementación en materia de SI). Por lo que establece la definición de las bases para futuras ejecuciones del proceso de gestión de riesgos. A su vez, busca la determinación de un apetito de riesgos corporativo (de no existir uno en la organización), con el objetivo de guiar a los responsables de aceptación de los riesgos de SI.

Entradas ("Inputs")

- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- Estadios de SI.
- Estructura preliminar de seguridad.
- Política de SI.
- Estructura de SI.
- Documentación de roles y autoridades de SI
- "*Requerimientos de SI*" [20] identificados anteriormente dentro del primer macroproceso de implementación.
- Apetito de riesgos de la organización (de existir).

Macroprocesos principales

La definición, estructura y mecanismos del presente macroproceso quedan supeditados al libre criterio de la organización, siempre y cuando cumpla con los requerimientos del MRU vinculados a su estadio de madurez objetivo.

Salidas ("Outputs")

- "*Documentación de la metodología de gestión de riesgos de SI*" [20].

- "*Documentación de los objetivos de control y controles*" [20] establecidos como tratamiento de riesgos de SI.
- "*Plan de tratamiento de riesgos*" [20].
- "*Documentación de aceptación de riesgos residuales*" [20].
- Documentación de aprobación de aceptación de riesgos residuales "*por parte del negocio*" [20].
- Apetito de riesgos de SI de la organización.

5. *Análisis Gap*

Objetivos

- Bajar a tierra el análisis estratégico de madurez de SI realizado anteriormente.
- Definir el "gap" de bajo nivel[33] de SI de la organización entre su situación actual y su situación objetivo.
- Establecer el input para el macroproceso de Construcción definitiva del Sistema de Mejora Continua, con el objetivo de conocer prioridades y necesidades de la organización que moldearán la estructura y requerimientos incluidos dentro del Sistema de Mejora Continua a diseñar.

Descripción

El foco principal del presente macroproceso estará puesto sobre la "bajada a tierra" del análisis de madurez realizado anteriormente. Esto se debe a que dicho análisis se corresponde con una actividad de nivel estratégico, por lo que los estadios de SI han sido establecidos en forma amplia y con un gran nivel de abstracción. El presente macroproceso tendrá un enfoque más gerencial/operativo relevando Dominio por Dominio y Área por Área del MRU con el objetivo de establecer la situación actual y futura objetivo individual de cada sección del marco de referencia. De esta forma, la organización conducirá un análisis del tipo "gap" entre lo existente y la visión de SI, para identificar los

[33] El gap de bajo nivel corresponde a los estratos operativos. Los cuales se encuentran debajo del estrato vinculado a la estrategia.

requerimientos faltantes algo indispensable para la construcción de su Sistema de Mejora Continua (lo cual configura el siguiente macroproceso dentro del flujo de trabajo).

Entradas ("Inputs")

- Análisis de madurez de SI.
- "*Documentación de los objetivos de control y controles*" [20] establecidos como tratamiento de riesgos de SI.
- "*Plan de tratamiento de riesgos*" [20].
- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- "*Requerimientos de SI identificados anteriormente dentro del primer macroproceso de implementación*" [20].
- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.
- Mapeo preliminar de requerimientos del MRU.

Macroprocesos principales

La definición, estructura y mecanismos del presente macroproceso quedan supeditados al libre criterio de la organización, siempre y cuando cumpla con los requerimientos del MRU vinculados a su estadio de madurez objetivo.

Salidas ("Outputs")

- Mapeo definitivo de requerimientos a implementar del MRU.
- Identificación de políticas y procesos a diseñar e implementar por la organización.
- Establecimiento definitivo de los estadios de madurez individuales de seguridad.
- Modificaciones a la estructura/mecanismos de gobierno de seguridad.

6. Construcción definitiva del Sistema de Mejora Continua

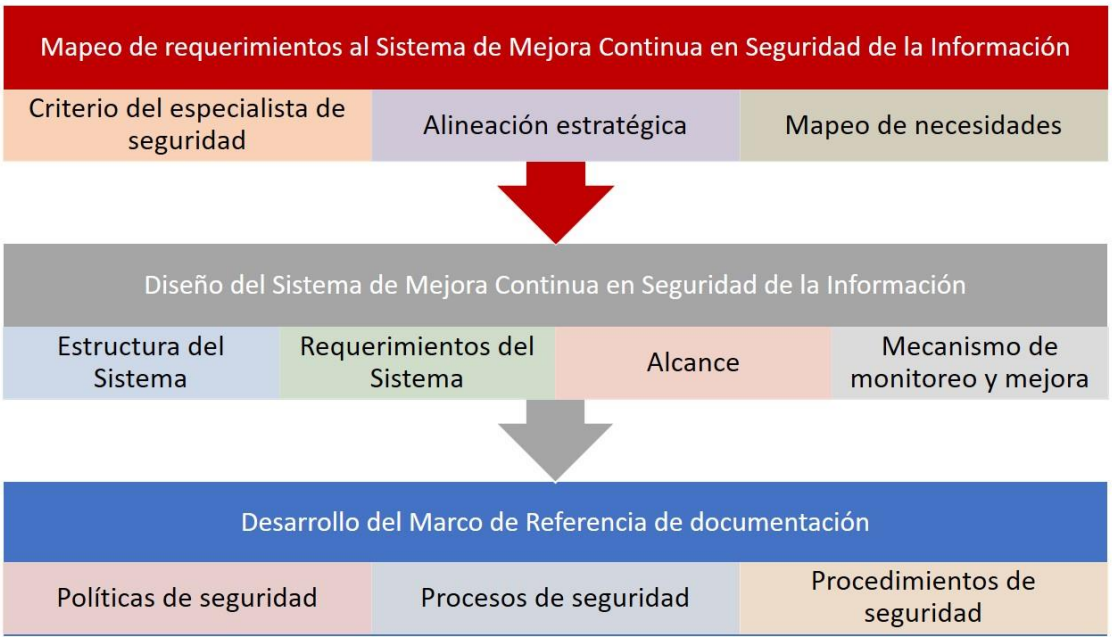

Ilustración 3.2.4: macroprocesos de nivel 2 que componen el macroproceso de nivel 1: Construcción definitiva del Sistema de Mejora Continua [20].

Objetivos

- "*Desarrollar un diseño del*" [20] Sistema de Mejora Continua en SI "*que sea único en su detalle para toda la organización*" [20]. Esta visión unificada evitará numerosos problemas de comprensión por parte de las diversas áreas o RRHH de la organización.
- "*Desarrollar la estructura y los requerimientos del*" [20] Sistema de Mejora Continua en SI "*en función tanto de las opciones de riesgos seleccionadas anteriormente como de los requerimientos a cumplir por la organización*" [20].

Descripción

El presente macroproceso se enfoca en completar el Sistema de Mejora Continua de la organización en forma definitiva, a través de establecer su estructura, delinear sus requerimientos, definir su alcance y establecer su mecanismo de monitoreo y mejora continua. El macroproceso rondará permanentemente la actividad de mapeo de

requerimientos del MRU con las necesidades de la organización, para así definir los controles, lineamientos, políticas, procesos y buenas prácticas del marco de referencia que implementará.

Entradas ("Inputs")

- "*Documentación de los objetivos de control y controles*" [20] establecidos como tratamiento de riesgos de SI.
- "*Plan de tratamiento de riesgos*" [20].
- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- "*Requerimientos de SI identificados anteriormente dentro del primer macroproceso de implementación*" [20].
- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.
- Mapeo definitivo de requerimientos a implementar del MRU.
- Identificación de políticas y procesos a diseñar e implementar por la organización.
- Estadios de madurez operativos de SI.
- Modificaciones a la estructura o a los mecanismos de gobierno de SI.
- "*Documentación de la metodología de gestión de riesgos de SI*" [20] de la organización.
- Inventario de activos de información de la organización (en función del alcance establecido para el proyecto).
- Documentación de "*la clasificación de los activos de información de la organización*" [20].
- "*Objetivos estratégicos de SI*" [20].

Macroprocesos principales

- Mapeo de requerimientos al Sistema Mejora Continua de la organización.
    - Mapeo de necesidades.
    - Alineamiento estratégico de requerimientos.
- Diseño del Sistema de Mejora Continua en SI.
    - Establecimiento de la estructura Sistema de Mejora Continua.
    - Definición de los requerimientos objetivo.
    - Diseño de los mecanismos de monitoreo y mejora del Sistema de Mejora Continua.
- "*Desarrollo del marco de referencia de documentación*" [20].
    - Identificación y desarrollo preliminar de las políticas de seguridad necesarias.
    - Identificación y desarrollo preliminar de los procesos de seguridad de alto nivel necesarios.
    - Identificación y desarrollo preliminar de los procesos de seguridad de bajo nivel necesarios.

Salidas ("Outputs")

- "*Declaración de aplicabilidad*" [20].
- "*Diseño definitivo del*" [20] Sistema de Mejora Continua en SI.
- "*Marco de referencia para la documentación del*" [20] Sistema de Mejora Continua en SI.
- "*Plantillas de documentación del*" [20] Sistema de Mejora Continua en SI.
- Mecanismos de monitoreo y mejora del Sistema de Mejora Continua.

Etapa 2: implementación

La presente etapa se encuentra conformada únicamente por los siguientes dos macroprocesos:

- Implementación del Sistema de Mejora Continua.
- Desarrollo e implementación del Programa de toma de conciencia, Entrenamiento y Difusión del MRU.

Se procederá a detallar su estructura y componentes a continuación.

1. *Implementación del Sistema de Mejora Continua*

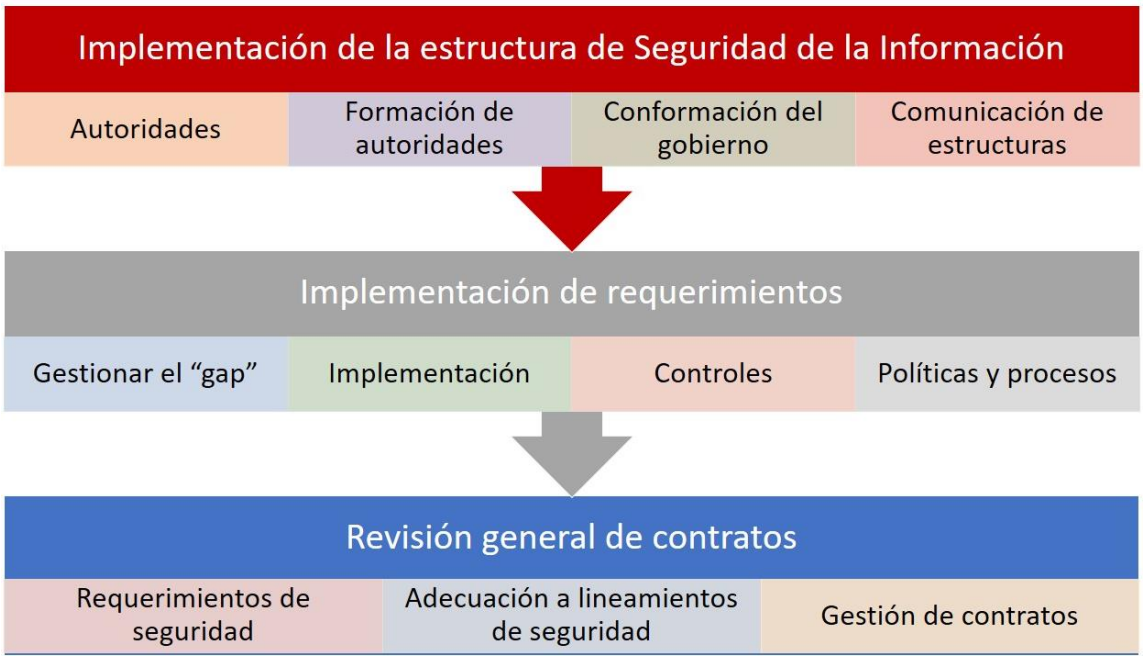

Ilustración 3.2.5: macroprocesos de nivel 2 que componen el macroproceso de nivel 1: Implementación del Sistema de Mejora Continua

Objetivos

- Bajada a tierra de las estructuras tanto gerenciales como de gobierno de SI.
- Establecimiento de las autoridades de SI.

- Planeamiento de adecuación a los requerimientos del MRU seleccionados anteriormente.
- Implementación de los requerimientos objetivo del MRU y del Sistema de Mejora Continua de la organización.

Descripción

El presente macroproceso se centra específicamente en "*implementar y operar controles y otras medidas enfocadas en el tratamiento de los riesgos* de *la SI*" [19] de la organización, con el objetivo final de implementar controles, políticas, procesos y procedimientos y lineamientos de SI, en función del análisis de madurez y mapeo de requerimientos realizados anteriormente.

Entradas ("Inputs")

- "*Declaración de aplicabilidad*" [20].
- "*Diseño definitivo del*" [20] Sistema de Mejora Continua en SI.
- "*Marco de referencia para la documentación del*" [20] Sistema de Mejora Continua en SI.
- "*Plantillas de documentación del*" [20] Sistema de Mejora Continua en SI.
- "*Documentación de los objetivos de control y controles*" [20] establecidos como tratamiento de riesgos de SI.
- "*Plan de tratamiento de riesgos*" [20].
- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.
- Identificación de políticas y procesos a diseñar e implementar por la organización.

- "*Documentación de la metodología de gestión de riesgos de SI*" [20] de la organización.
- Inventario de activos de información de la organización (en función del alcance establecido para el proyecto).

Macroprocesos principales

- Implementación de la estructura de SI.
  - Nombramiento de autoridades de SI.
  - Formación específica de las autoridades de SI.
  - Conformación de los organismos de gobierno de SI.
  - Comunicación y documentación de la estructura de seguridad.
- Implementación de requerimientos.
  - Gestión del "gap" y elaboración del plan de adecuación.
  - Implementación de controles y lineamientos de seguridad.
  - Implementación de políticas de seguridad.
  - Implementación de procesos de seguridad.
  - Diseño del sistema de Seguridad Física de la organización.
  - Diseño del sistema de gestión de la capacidad y seguridad de TICs de la organización.
- Revisión general de contratos (adecuación de estos a las nuevas directivas de SI de la organización).
  - Gestión de lineamientos de seguridad dentro de contratos.
  - Adecuación de contratos.

Salidas ("Outputs")

- Acta de nombramiento de autoridades de SI.
- Documentación del establecimiento de los organismos de gobierno de SI.
- Planes de adecuación a los requerimientos del MRU.
- Marco de Referencia de lineamientos de SI de contratos y acuerdos de la organización.

2. *Desarrollo e implementación del Programa de toma de conciencia, Entrenamiento y Difusión del MRU*

Objetivos

- Desarrollo y planeamiento de todas las acciones y procesos de capacitación y formación de los RRHH de la organización y usuarios de terceras partes.
- Implementación de las acciones de conciencia, entrenamiento y difusión de la SI planificadas.
- Monitoreo y revisión de todas las acciones de conciencia, entrenamiento y difusión de la SI.

Descripción

Macroproceso enfocado en el desarrollo y posterior implementación del Programa de toma de Conciencia, Entrenamiento y Difusión del MRU. Para mayor detalle de los requerimientos de dicho programa, favor de referirse al Subsistema de Seguridad de Gestión de Recursos Humanos.

Entradas ("Inputs")

- "*Documentación de los objetivos de control y controles*" [20] establecidos como tratamiento de riesgos de SI.
- "*Plan de tratamiento de riesgos*" [20].
- "*Definición del alcance del proyecto*" [20].
- "*Listado de todas las partes interesadas vinculadas al proyecto*" [20].
- "*Documentación de los objetivos y prioridades de SI de la organización*" [20].
- "*Requerimientos de SI identificados anteriormente dentro del primer macroproceso de implementación*" [20].
- Política de SI.
- Política de gobierno SI.
- Marco de referencia de gobierno SI.
- Estructura de SI.

- Estadios de madurez operativos de SI.
- "*Documentación de la metodología de gestión de riesgos de SI*" [20] de la organización.
- Inventario de activos de información de la organización (en función del alcance establecido para el proyecto).
- Documentación de "*la clasificación de los activos de información de la organización*" [20].
- "*Objetivos estratégicos de SI*" [20].
- "*Declaración de aplicabilidad*" [20].
- "*Diseño definitivo del*" [20] Sistema de Mejora Continua en SI.
- "*Marco de referencia para la documentación del*" [20] Sistema de Mejora Continua en SI.
- "*Plantillas de documentación del*" [20] Sistema de Mejora Continua en SI.

Macroprocesos principales

La definición, estructura y mecanismos del presente macroproceso quedan supeditados al libre criterio de la organización, siempre y cuando cumpla con los requerimientos del MRU vinculados a su estadio de madurez objetivo (fundamentalmente aquellos vinculados al Subsistema de Seguridad de Gestión de los Recursos Humanos).

Salidas ("Outputs")

- "*Materiales del*" [20] Programa de toma de Conciencia, Entrenamiento y Difusión del MRU.
- "*Establecimiento y documentación de las responsabilidades, roles y facultades del*" [20] Programa de toma de Conciencia, Entrenamiento y Difusión del MRU.
- "*Planes de*" de toma de Conciencia, Entrenamiento y Difusión del MRU [20].
- Metodología de toma de Conciencia, Entrenamiento y Difusión del MRU.

Etapa 3: monitoreo & revisión

La definición, estructura y mecanismos de los macroprocesos de la presente sección quedan supeditados a los lineamientos establecidos por los requerimientos del MRU vinculados a estos. Favor de referirse al Subsistema de Seguridad de Seguimiento & Control, para mayor detalle sobre los mismos).

Los macroprocesos involucrados configuran los siguientes:

- "*Monitoreo y revisión de la performance y efectividad del*" [19] Sistema de Mejora Continua en SI de la organización.
- Auditoria del Sistema de Mejora Continua.
- Mantenimiento del Sistema de Mejora Continua.
- Revisión gerencial del Sistema de Mejora Continua.
- Desarrollo, implementación y monitoreo de métricas de SI.

Etapa 4: actuar

La definición, estructura y mecanismos de los macroprocesos de la presente sección quedan supeditados a los lineamientos establecidos por los requerimientos del MRU vinculados a estos. Favor de referirse al Subsistema de Seguridad de Seguimiento & Control, para mayor detalle sobre los mismos).

Los macroprocesos involucrados configuran los siguientes:

- "*Implementación de la mejora continua*" [19].
- Diseño, implementación, monitoreo y mantenimiento de mejoras al Sistema de Mejora Continua.

Los macroprocesos detallados anteriormente conforman una guía de implementación para todo aquel profesional de seguridad que pretenda adherir su organización al MRU, a través del diseño e implementación del Sistema de Mejora Continua en SI. Debido a que estos macroprocesos únicamente conforman una guía del camino a seguir, su nivel de abstracción es significativo, a razón de permitir su adecuación a cualquier tipo de organización. Esta es la razón por la cual el macroproceso de implementación del Sistema de Mejora Continua conforma un macroproceso de tipo genérico.

¿Por qué un macroproceso genérico? El motivo se basa fundamentalmente en que cada organización posee una naturaleza propia (una cultura específica, una estructura determinada, sus propios objetivos estratégicos, un mecanismo de gobierno determinado, entre otros aspectos) a la cual debe amoldarse el macroproceso de implementación. Sería ingenuo el intento inverso de amoldar la naturaleza de la organización al macroproceso de implementación. Es por esa razón, que el macroproceso de implementación del Sistema de Mejora Continua establece únicamente las bases del camino a seguir con un gran nivel de abstracción. Enfocándose únicamente en convertirse en una guía estratégica y evitando la necesidad de disminuir el nivel de abstracción hacia una guía operativa (lo cual podría provocar inconsistencias con la naturaleza de la

organización, su apetito de riesgo, su estructura y/o sus propios procesos de negocio ya definidos o en funcionamiento).

[Página dejada en blanco intencionalmente]

4

Próximos pasos

Debido a la ya gran extensión que ha tomado el presente TFM, se ha optado por dejar de lado la inclusión de un número limitado de normas, estándares y marcos de referencia en materia de SI. No obstante, dicha documentación fuente ha sido identificada y analizada preliminarmente con el objetivo de incluirlas dentro de una futura nueva versión del MRU. Se incluye a continuación una lista de dicha documentación fuente:

- ISO 31.010, con el objetivo de adicionar los lineamientos fundamentales de dicha norma al Subsistema de Seguridad de Gestión de Riesgos.
- Normas SP-800 del NIST (Instituto Nacional de Estándares y tecnología de los Estados Unidos de América), con el propósito de agregar múltiples lineamientos y buenas prácticas a la gran mayoría de Subsistemas de SI del MRU.
- ISO 55.001[34] (norma internacional de gestión de activos), con el objetivo de adicionar los lineamientos fundamentales de dicha norma al Subsistema de Seguridad Lineamientos de Seguridad (específicamente dentro del Área de Seguridad LS2.3).
- ISO 27.032 (norma internacional de ciberseguridad), con el objetivo de adicionar los lineamientos fundamentales de dicha norma a la gran mayoría de Subsistemas de SI del MRU.

[34] Dicha norma "*se centra en desarrollar un sistema de gestión del ciclo de vida de activos*" con el objetivo de "*optimizar la gestión de los activos y*" colaborando en el cumplimiento de "*los requisitos de seguridad y rendimiento necesarios*" [22].

- ISO 9.001 (norma internacional de calidad), con el objetivo de adicionar ciertos lineamientos del sistema de gestión de calidad al gobierno de SI y a los mecanismos de diseño, modelado, implementación y mejora de procesos de seguridad.
- Guías técnicas de la NSA (Agencia Nacional de Seguridad de los Estados Unidos de América) y el DHS (Departamento de Seguridad Nacional de los Estados Unidos de América), con el objetivo de dotar al MRU de número significativo de buenas prácticas en la materia con un reducido nivel de abstracción y con un relativo sesgo hacia el campo técnico de la seguridad.
- Lineamientos completos del estándar de buenas prácticas del ISF [4] y del Marco de Trabajo COBIT [5].

A su vez, se han dejado de lado un número limitado de iniciativas de modificación o adhesión de requerimientos, lineamientos y nuevos conceptos en materia de SI al MRU debido al mismo motivo, relativo al alcance del TFM, detallado anteriormente. Entre las iniciativas planeadas para la próxima versión del marco de referencia podemos encontrar:

- Análisis global de los requerimientos del MRU en función de los lineamientos de la norma ISO 27.006 [21], lo que facilitará la tarea de los auditores de seguridad que deben certificar la adhesión a la norma ISO 27.001 [1].
- La inclusión del concepto de Ciclos de vida de SI, en función de los lineamientos emanados de la norma ISO 27.001 [1] y la guía de buenas prácticas del ISF [4]. Los ciclos de vida fundamentales a implementar serían los siguientes:
    - Ciclo de vida de la información, el cual implementaría un proceso circular (no lineal), global y unificado para la gestión de toda la información vinculada a la organización. De esta forma, se facilitaría significativamente la implementación de acciones de SI y su correspondiente supervisión y monitoreo.
    - Ciclo de vida del gobierno de SI.
    - Ciclo de vida de políticas de SI.

- Ciclo de vida de Hardware, con el objetivo de separar la gestión del hardware del común de los dispositivos o medios de la organización. Esto permitirá el diseño e implementación de lineamientos, políticas y procedimientos específicos de SI, enfocados y adaptados exclusivamente al manejo, uso, mantenimiento y disposición del hardware.
- Ciclo de vida del empleo (RRHH), con el objetivo de proveer mayor importancia al proceso clave de gestión de los RRHH durante la implementación y ejecución del Sistema de Mejora Continua en SI. El MRU le brinda una significativa importancia a la correcta comunicación, formación e involucramiento constante de los RRHH de la organización dentro de las iniciativas, proyectos y procesos ese SI.
- Ciclo de vida de Activos de Información.
- Ciclo de vida de Contratos, SLAs y requerimientos (Compliance), el cual se encargará de gestionar que los contratos y acuerdos de nivel de servicio cumplan permanentemente con todos los lineamientos y disposiciones de SI (tanto internas de la organización como externas dadas por leyes, regulaciones o lineamientos del mercado).

- Adhesión de un Subsistema o Área de Seguridad destinada a incorporar un área de compliance de la SI, que se encargue de la revisión gerencial de la seguridad global de la organización. Lo cual modificaría el esquema de la estructura general de seguridad a partir del estadio de madurez “C”.
- Separación de los requerimientos del MRU en distintos documentos, en función de los diversos estadios de madurez de SI. De esta forma, cada nivel de madurez tendría su propio documento de implementación.
- Diseño, identificación e implementación de requerimientos especiales. Para mayor información, favor de referirse al Anexo I del presente trabajo.

[Página dejada en blanco intencionalmente]

5

Conclusiones

La realización del presente trabajo requirió del diseño e incorporación de una serie de mejoras al Marco de Referencia Unificado en SI (MRU) con el objetivo de:

- Mejorar la versión piloto del MRU, al realizar mejoras a los Subsistemas de Seguridad pilotos incorporados dentro del TFE.
- Simplificar la compleja tarea de implementación del MRU al desarrollar un macroproceso de implementación, enfocado en proveer una guía que facilite el trabajo de adhesión al MRU por parte de los especialistas en seguridad.
- Facilitar la visualización de la "bajada a tierra" de la estrategia del MRU, a través de la incorporación del concepto de "capas de seguridad".
- Incorporación de buenas prácticas, con el enfoque puesto en completar los Subsistemas de Seguridad faltantes.
- Mejorar el Modelo de Madurez de SI.
    - Ajustando los lineamientos individuales de cada estadio de madurez.
    - Adicionando lineamientos a los estadios de madurez.
    - Modificando y simplificando su estructura y metodología de uso y denominación de los niveles de madurez.
- Flexibilizar las tareas de adhesión a los estadios de madurez del MRU.
    - Incorporando el concepto de "saltos de madurez".
    - Flexibilizando los requerimientos necesarios para alcanzar estadios intermedios.
    - Incorporando los conceptos de "estadio general" y "estadios individuales" de madurez de SI.

La estrategia del MRU se centra fundamentalmente en combinar, centralizar y crear una complementación e integración entre toda la documentación fuente considerada por el presente trabajo. Para generar así una sinergia única entre los diversos requerimientos del Sistema de Mejora Continua en SI. Adicionando a esta sinergia de buenas prácticas, el MRU logra a su vez simplificar el camino a recorrer por parte de las organizaciones en forma significativa. Esto se debe a que facilita la comprensión y relevamiento de la documentación fuente más reconocida en la materia. ¿Cómo lo hace? A través de la clasificación global de todos sus requerimientos de seguridad en función del Modelo de Madurez de SI, lo cual permite a las organizaciones el diseño efectivo y satisfactorio de medidas e iniciativas de SI encausadas en un gran camino a seguir zanjado por el Modelo de Madurez del MRU.

Por lo tanto, el MRU logra satisfactoriamente:

- "*Convertirse en una fuente de conocimientos libre y gratuita para cualquier profesional vinculado a la SI*" [2].
- Derribar la complejidad "*ante la cual todos los profesionales de SI se encuentran a la hora de alcanzar la mejora continua*" [2], por medio del diseño de un camino a seguir acompañado por metodologías y lineamentos genéricos de gestión de SI.
- "*Llevar a un nivel único en la materia los principios 3 y 4 del marco teórico COBIT*" [2]:
    - "*Aplicar un Marco de Referencia Único Integrado*" [5].
    - "*Hacer posible un Enfoque Holístico*" [5].

[Página dejada en blanco intencionalmente]

6

Bibliografía

Se incluye a continuación el detalle de toda la bibliografía que ha sido incorporada tanto textualmente como a modo de referencia dentro del presente TFM.

[1] Instituto Argentino de Normalización y Certificación, **Proyecto 1 de IRAM-ISO/IEC 27.001:2015 Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la SI – Requisitos (ISO/IEC 27001:2013, IDT),** IRAM, 2015.

[2] Lucas Falivene, **Marco de Referencia Unificado en Seguridad de la Información**, Universidad de Buenos Aires - Facultad de Ciencias Económicas, 2018.

[3] Consejo de la Unión Europea, **Directiva 2008/114/CE: identificación y designación de infraestructuras críticas europeas y evaluación de la necesidad de mejorar su protección**, Consejo de la Unión Europea, 2008.

[4] Information Security Forum, **The Standard of Good Practice for Information Security 2016**, Information Security Forum Limited, 2016.

[5] ISACA, **COBIT 5 para SI**, ISACA, 2012.

[6] International Organization for Standardization, **ISO 31.000:2009 Risk management - Principles and guidelines**, ISO, 2009.

[7] International Organization for Standardization, **ISO/IEC FDIS 27.014:2012 Information technology – Security techniques – Governance of information security**, ISO/IEC, 2012.

[8] International Organization for Standardization, **ISO/IEC 27.000:2005 Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary**, ISO/IEC, 2009.

[9] Organization for Economic Co-operation and Development (OECD), **Digital Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document**, OECD Publishing, 2015.

[10] Raúl Saroka y Mara Irene Misto Macías, **Material brindado durante la cátedra de Gestión Estratégica de la Seguridad Informática dentro de la Maestría en Seguridad Informática de la UBA**, UBA - FCE, 2017.

[11] Instituto Argentino de Normalización y Certificación, **IRAM-NM ISO/IEC 27.005:2012 Tecnología de la información – Gestión del riesgo de la SI**, IRAM, 2012.

[12] Instituto Argentino de Normalización y Certificación, **IRAM-ISO/IEC 27.007:2014 Tecnología de la información – Técnicas de seguridad**, IRAM, 2014.

[13] EAFIT.edu.co, **Nota de Clase 10 Medidas de Tratamiento del Riesgo**, http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/Nota%20de%20Clase%2010%20Medidas%20de%20Tratamiento%20del%20Riesgo.pdf (consultada el 24/01/2019).

[14] International Organization for Standardization, **ISO/IEC 27.002:2013 Information technology – Security techniques – Code of practice for information security controls**, ISO/IEC, 2013.

[15] Instituto Argentino de Normalización y Certificación, **Esquema 1 de Norma IRAM-ISO/IEC 27.004 – Tecnología de la información – gestión de la SI – medición**, IRAM, 2010.

[16] International Organization for Standardization, **ISO/IEC 19.011:2011 Guidelines for auditing management systems**, ISO, 2011.

[17] Gartner, IT Glossary, https://www.gartner.com/it-glossary/best-of-breed/ (consultada el 13/2/2019).

[18] Tom Scholtz & F. Christian Byrnes, **Use Information Security Program Maturity Timeline as an Analysis Tool**, Gartner, 2005.

[19] International Organization for Standardization, **ISO/IEC 2nd DIS 27003:2016 2010 Information Technology – Security techniques – Information security management system – guidance**, ISO/IEC, 2016.

[20] International Organization for Standardization, **ISO/IEC 27003:2010 Information Technology – Security techniques – Information security management system implementation guidance**, ISO/IEC, 2010.

[21] International Organization for Standardization, **ISO/IEC 27.006:2007 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems**, ISO/IEC, 2007.

[22] bsi group, **¿Qué es la ISO 55001? Sistema de Gestión de activos**, https://www.bsigroup.com/es-ES/PAS-55-Gestion-de-activos (consultada el 22/03/19).

[23] National Security Agency, **Metodología de SI de la NSA**, NSA.

[24] G&P, imágenes obtenidas, http://www.gpqm.com/services/, (consultada el 02/08/2017).

[25] Uptime Institute, **Data Center site infrastructure TIER standard: topology**, Uptime Institute Professional Services, 2009.

[26] Uptime Institute, **Data Center site infrastructure TIER standard: operational sustainability**, Uptime Institute Professional Services, 2010.

[27] International Organization for Standardization, **ISO/IEC 22.301:2012 Societal Security – Business continuity management systems - Requirements**, ISO/IEC, 2012.

[28] Definición brindada por el diccionario que la compañía Google posee disponible a través de su buscador.

[Página dejada en blanco intencionalmente]

7

Glosario

Se incluye a continuación tanto la nómina de definiciones clave como de definiciones especiales que han sido utilizadas a lo largo del desarrollo del presente TFM, las cuales sin duda alguna colaboraran en la lectura y entendimiento de este por parte del lector.

7.1 Nómina de definiciones clave

Documentación fuente: dicho concepto incluye a todos los estándares, normas, marcos teóricos, manuales y guías internacionales, regionales y nacionales de SI que han sido consultados y analizados para la realización del presente trabajo [2]. La documentación fuente ha sido incorporada como el principal input del MRU, por lo que en gran medida dicho marco de referencia constituye una centralización y consolidación de todos los documentos que componen la documentación fuente.

Requerimiento: todo control, proceso, política, medida, lineamiento, procedimiento, buena práctica o acción de SI requerida por el MRU. Conforman el elemento de menor jerarquía y fundamental del MRU. Dichos requerimientos son los que conforman los Subsistemas, Áreas y Dominios de SI.

MRU: Las siglas MRU hacen referencia al Marco de Referencia Unificado en SI. El objetivo fundamental tanto del presente TFM como del TFE se ha centrado en la conformación de dicho Marco de Referencia Unificado en SI a través de la centralización y consolidación de

toda la documentación fuente dentro de un Modelo de Madurez de SI. Dicha metodología logra brindar una sinergia única entre los componentes de dicho marco de referencia, favoreciendo y simplificando así la comprensión de los lineamientos del MRU y su correspondiente implementación por parte de los especialistas en SI. La siguiente ilustración muestra los diferentes componentes del MRU tal y como han sido diseñados y detallados durante el TFM [2].

Ilustración 8.1.1: componentes del MRU [2].

Modelo de Madurez de SI (MMSI): *"conforma el objetivo primordial del **MRU**, siendo una guía holista y práctica para que cualquier tipo de organización pueda navegar de forma simple desde los niveles iniciales del mismo, hasta alcanzar la mejora continua en SI. Su objetivo es guiar y apoyar a la organización antes, durante y después de la implementación del Sistema de Mejora Continua en SI"* [2].

Sistema de Mejora Continua en SI (SMCSI): *"implementado por el **MRU**. El mismo contiene todos los requerimientos (controles, buenas prácticas, procesos, procedimientos, políticas y lineamientos) del **MRU**. Se encuentra dividido en 9 grandes Subsistemas de SI"* [2].

Subsistema de SI: "*conforma los subgrupos en los que los distintos requerimientos del Sistema de Mejora Continua en SI se encuentran clasificados y organizados*" [2].

SOO[35] [2]: *Gerente Operativo de Seguridad*, responsable del día a día de la SI, ya que es quien lleva adelante los procesos tácticos y operativos de seguridad (gestión de incidentes, supervisión e implementación de controles, políticas y procesos de SI). Dicho responsable complementa al accionar del CISO, quien se focaliza en aquellos procesos estratégicos de SI de la organización. Conforma una de las áreas de Seguridad requeridas por el Sistema de Mejora Continua del MRU. Establecido por el requerimiento LS2.1.10 [2]. Requerido a partir del nivel de madurez "C" [2].

RASI [2]: *Responsable de Auditoria de SI*. Establecido por el requerimiento LS2.1.5. Requerido a partir del nivel de madurez "C" [2].

RG [2]: *Responsables Gerenciales*, todo aquel gerente o titular de un área, división o sección de la organización. Establecidos por el requerimiento LS2.1.12. Requeridos a partir del nivel de madurez "C" [2].

RMO[36] [2]: responsable de riesgos de SI de la organización. Conforma una de las áreas de SI requeridas por el SMCSI. Establecido por el requerimiento LS2.1.8. Requerido a partir del nivel de madurez "C" [2].

RP [2]: *Responsable de Proceso*, aquellos responsables por la eficiente y eficaz ejecución de un proceso. Son a su vez responsables por el mantenimiento, revisión y mejora continua del mismo. Establecidos por el requerimiento LS2.1.4 [2]. Requeridos a partir del nivel de madurez "C" [2].

CIPO[37] [2]: *Responsable de Procesos y Mejora Continua de SI* de la organización. Su trabajo se basa en el estado futuro de la seguridad y no en las operaciones diarias de SI. Conforma una de las áreas de seguridad requeridas por el MRU. Establecido por el requerimiento

[35] "*Security Operations Office*", Oficina de Operaciones de Seguridad por sus siglas en inglés.
[36] *"Risk Management Office"*, Oficina de Gestión de Riesgos por sus siglas en inglés.
[37] *"Continuous Improvement & Process Office"*, Oficina de Procesos y Mejora Continua por sus siglas en inglés.

LS2.1.9 y complementado por el requerimiento LS2.1.14 [2]. Requerido a partir del nivel de madurez "C" [2].

7.2 Nómina de definiciones generales

Acciones correctivas: "*acción realizada para eliminar la causa de una no conformidad y para prevenir su recurrencia*" [8].

AES: "*Áreas de Extrema Seguridad, establecidas por el* ***MRU****. A diferencia de la norma ISO 27.001, que plantea controles genéricos aplicables a cualquier tipo de organización*" [2] "*independientemente de su tipo, tamaño o naturaleza*"[38] [1], "*ciertos requerimientos del* ***MRU*** *no son genéricos y pueden constituir medidas extremadamente excesivas y agresivas para la naturaleza del negocio de determinadas organizaciones. Por este motivo, dichos requerimientos serán considerados como extras para el común de las organizaciones y, solo serán necesarios para declarar conformidad para aquellas áreas o sectores críticos a los cuales no todas las organizaciones se encuentran vinculadas. Dichos sectores o áreas críticos serán denominados por el MRU como Áreas de Extrema Seguridad y conforman las siguientes:*" [2]

a. "*Investigación y desarrollo*" [2].
b. "*Organizaciones contratistas de sectores sensibles de gobiernos*" [2].
c. "*Sectores vinculados al resguardo de la composición, estructura y/o detalle de productos únicos y originales no patentados*" [2].
d. "*Áreas vinculadas a los sectores de defensa y seguridad*" [2].
e. "*Cualquier organización categorizada como una infraestructura crítica en función de la Directiva 2008/114/CE del Consejo de la Unión Europea [3]*" [2].

[38] En función de lo establecido en la sección 1, página 8 de la Norma IRAM-ISO/IEC 27.001:2015 [1].

AI: *Activo de Información*, conforma cualquier objeto que tenga valor para la organización [41] [8].

Ataque: "*Intento de destruir, exponer, alterar, inhabilitar, robar o ganar acceso no autorizado o hacer uso no autorizado de cualquier activo de información de la organización*" [4].

Autenticación: "*la provisión de garantía de que una característica reclamada por una entidad es correcta*" [8].

Autenticidad: "*propiedad que establece que una entidad es quien dice ser*" [8].

BPM: Gestión de Procesos de Negocio, por sus siglas en inglés.

CEP: Comité Ejecutivo Permanente, se encarga de analizar, diseñar, debatir y aprobar nuevos procesos, procedimientos, guías y normas derivadas de las políticas aprobadas por el CSI.

CISO[39]: Gerente de SI, autoridad máxima de SI en la organización.

Confidencialidad: "*propiedad de la información que determina que la misma no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados*" [8], para lo cual se debe de "*preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria*" [5].

Conformidad: "*cumplimiento de un requisito*" [8] del MRU.

Control: *"medida que modifica riesgo"* [6].

Control: "*medida que modifica riesgo*" [8]. Pueden ser "*procesos, políticas, dispositivos, practicas o cualquier otro tipo de acción que modifica riesgo"* [8].

Criterio de riesgo: apetito de riesgos de la organización. Definido por el órgano rector de gobierno de la organización. Su objetivo es ser utilizado por la dirección ejecutiva como inputs en su toma de decisiones para que las actividades y acciones emprendidas por la

[39] "*Chief Information Security Oficer"*, Gerente de Seguridad de la Información por sus siglas en inglés.

organización en general se encuentren alineadas con el apetito (aversión a riesgos) establecido por el sistema de gobierno de la organización.

CSI: Comité de SI, se encarga de coordinar las actividades estratégicas de SI en toda la organización y del establecimiento de las diversas políticas de SI de la organización.

Dirección ejecutiva: Persona o grupo de personas que tienen la responsabilidad brindada por el órgano rector de gobierno de la organización para la construcción, ejecución, implementación y control de las estrategias y políticas, diseñadas por este último, que permitirán lograr la misión de la organización. La dirección ejecutiva de la organización incluye al CEO, CFO, COO, CIO, CISO y todos aquellos roles de similares características [7] [1] [5].

Disponibilidad: "*propiedad de la información que determina que esta se encuentra accesible y utilizable*" [8] "*de manera confiable y en el momento oportuno" [5] "a petición de una entidad autorizada*" [8].

EGR: Equipo de Gestión de Riesgos, responsable por la "*evaluación, control, optimización, financiación y monitorización del riesgo de SI con el propósito de incrementar el valor de la organización a corto y largo plazo para las partes interesadas*" [5].

Gestión de riesgos: "*actividades coordinadas para dirigir y controlar*" [6] la forma en que la organización toma sus decisiones y plica sus recursos para el logro de sus objetivos estratégicos.

Gobierno de SI: Sistema que controla y dirige las actividades de SI de la organización, a través del establecimiento de un marco de acción y gestión [8] [12].

Hardware: "*Cualquier activo físico utilizado para dar soporte a la información o sistemas de la organización*". [4]

Información documentada: "*la información que debe de ser controlada y mantenida por una organización y, el medio en el que la misma está contenida*" [8].

Información: aplica a todo conjunto de datos producido, recibido u obtenido por la organización. Existe en diversas formas (tanto sea digital, escrita, hablada, transmitida o visualizada) [11] [1] [12].

Instalaciones de procesamiento de información: "*identifica cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo aloja*" [11].

Integridad: "*significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio, la autenticidad*" [5], "*la exactitud y la completitud de la información*" [11].

KPI: *Indicador Clave de Performance* por sus siglas en inglés ("*Key Performance Indicator*"), conforma una herramienta o método de medición del desempeño de la gestión. En este caso será utilizado para medir la performance de la gestión de SI.

Mejora continua: "*actividad recurrente para mejorar la performance de la organización*" [1].

MRE [2]: Marco de Referencia del MRU. Conforma el marco establecido y utilizado por el MRU para poder "*bajar a tierra*" la estrategia del MRU (detallada en el capítulo 2 del TFE). Se encuentra conformado por 6 niveles que facilitan el alineamiento de los requerimientos de SI del MRU con la propia estrategia del marco de referencia. Dicho Marco de Referencia, se encuentra basado en la metodología de "*cascada de metas*" utilizada por COBIT [5] para facilitar la navegación desde los principios estratégicos rectores del MRU hasta la implementación de los procesos de SI. Se encontrará mayor detalle sobre el Marco de Referencia dentro de la sección 3.4 del TFE [2].

No conformidad: "*incumplimiento de un requisito*" [16] del MRU.

Órgano rector de gobierno de la organización: persona o grupo de personas (consejo de directores, de administración o equivalente) que tienen la responsabilidad por el rendimiento, la estrategia y la visión de la organización. "*Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se*

alcanzan los" [5] objetivos estratégicos, "*establece la dirección de la organización a través de la priorización y la toma de decisiones y mide el rendimiento y cumplimiento respecto a la dirección y objetivos planificados*" [5].

Partes interesadas: término utilizado para referirse a todos aquellos que son afectados o pueden ser afectados por las actividades de una organización. Las partes interesadas internas consisten en los empleados, gerentes y propietarios. En cuanto a los externos se incluyen a los clientes, proveedores, Gobierno, acreedores, organizaciones públicas y privadas y la sociedad [5] [8] [12].

PCED: Programa de toma de Conciencia, Entrenamiento y Difusión del MRU. El mismo se establece dentro del Subsistema de SI Recursos Humanos (referirse a la sección RH2 del MRU).

PSI: Política de SI.

RASI: Responsable de Auditoria de SI, corresponde a una de las autoridades de SI establecidas por el MRU.

Riesgo residual: *"riesgo remanente luego de haber realizado el correspondiente tratamiento de riesgo"* [6].

Riesgo: "*una desviación de lo esperado (positiva o negativa)"* que genera *"incertidumbre sobre"* el logro de *"los objetivos*" de la organización [6].

SI: "*asegura que dentro de la*" organización, "*la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)*" [5]. A su vez, conforma una actividad dedicada a la protección del valor generado por la organización a través de la disminución a un nivel aceptable de los riesgos a los cuales los activos de información de la organización se encuentran sujetos [8] [1].

SI: Seguridad de la Información.

Sistemas de información: "*aplicaciones, servicios, activos de TI y cualquier otro componente utilizado para manipular información*" [8].

SMCSI: Sistema de Mejora Continua en SI.

TI: Tecnología de la Información. Denota al área funcional y a la temática de tecnología y sistemas de información.

Vulnerabilidad: "*debilidad de un AI o un control que puede ser explotada por una o más amenazas*" [8].

[Página dejada en blanco intencionalmente]

Anexo I

Desarrollo del MRU

El presente capítulo del TFM se enfocará en establecer los 7 restantes Subsistemas de SI, que corresponden a aquellos no diseñados durante el TFE. De esta forma, el presente trabajo pretende dar un cierre al MRU al completar todos sus diversos requerimientos hasta el nivel de madurez "C". Por lo tanto, se incluirán a continuación ciertas secciones del presente trabajo que sin duda alguna facilitarán la lectura de los diferentes requerimientos de SI del MRU. Dichas secciones harán hincapié tanto en la terminología y metodología utilizada por el autor como el formato y la estructura de los Subsistemas de SI.

AI.1 Abreviaturas y conceptos más importantes utilizados por del MRU

Durante la realización de los Subsistemas piloto (Gobierno de SI y Lineamientos de SI [2]) y los Subsistemas complementarios del MRU, se han utilizado diversos atajos y conceptos dentro del desarrollo de los requerimientos de SI. Se incluyen a continuación aquellos considerados claves para facilitar la comprensión por parte del lector de los nuevos requerimientos diseñados como parte del TFM. No obstante, se podrá encontrar la nómina completa de definiciones generales dentro del glosario del presente trabajo.

Documentación fuente: dicho concepto incluye a todos los estándares, normas, marcos teóricos, manuales y guías internacionales, regionales y nacionales de SI que han sido consultados y analizados para la realización del presente trabajo [2]. La documentación fuente ha sido incorporada como el principal input del MRU, por lo que en gran medida

dicho marco de referencia constituye una centralización y consolidación de todos los documentos que componen la documentación fuente. Favor de referirse a la sección 1.6 del presente trabajo para encontrar mayor detalle sobre este concepto.

Requerimiento: todo control, proceso, política, medida, lineamiento, procedimiento, buena práctica o acción de SI requerida por el MRU. Conforman el elemento de menor jerarquía y fundamental del MRU. Dichos requerimientos son los que conforman los Subsistemas, Áreas y Dominios de SI.

CSI [2]: *Comité de SI*, se encarga de coordinar las actividades estratégicas de SI en toda la organización y del establecimiento de las diversas políticas de SI de la organización. Establecido por el requerimiento GOB1.4.5 y complementado por los requerimientos GOB 1.4.6, GOB1.4.7, GOB1.4.11 y GOB1.4.13 [2]. Requerido a partir del nivel de madurez "C" [2].

CEP [2]: *Comité Ejecutivo Permanente*, se encarga de analizar, diseñar, debatir y aprobar nuevos procesos, procedimientos, guías y normas derivadas de las políticas aprobadas por el CSI (Comité de SI). Es establecido por el requerimiento LS1.2.10 y complementado por los requerimientos LS1.3.8, LS1.3.9, LS2.2.3 y LS2.2.4 [2]. El CEP conforma uno de los componentes de gobierno de SI y solo es requerido a partir del nivel de madurez "B" [2].

CISO[40]: *Gerente de SI*, autoridad máxima de SI en la organización. Es establecido por el requerimiento GOB1.4.2 y complementado por los requerimientos GOB 1.4.3, GOB1.4.4, GOB1.4.10 y GOB1.4.12 [2].

EGR [2]: *Equipo de Gestión de Riesgos*, responsable por la "*evaluación, control, optimización, financiación y monitorización del riesgo de SI de la organización con el propósito de incrementar el valor de esta a corto y largo plazo para las partes interesadas*" [5]. Establecido por el requerimiento LS2.2.1 [2]. Requerido a partir del nivel de madurez "D" [2].

[40] "*Chief Information Security Oficer*", Gerente de Seguridad de la Información por sus siglas en inglés.

PCED: Programa de toma de Conciencia, Entrenamiento y Difusión del MRU. El mismo comprende un elemento fundamental en el éxito de las implementaciones de SI. Se encuentra establecido dentro del Subsistema de Seguridad de Recursos Humanos (referirse a RH2). Requerido a partir del nivel de madurez "C" [2].

PSI [2]: Política de SI. Establecida por el requerimiento LS1.2.1 [2].

SMCSI [2]: *Sistema de Mejora Continua en SI*. El mismo establece todos los requerimientos necesarios (procesos, políticas, protocolos, controles, metodologías, soluciones, lineamientos y buenas prácticas de seguridad) para que cualquier organización pueda, en función del MRU, alcanzar la mejora continua en SI. Detallado y establecido en el capítulo 3 del TFE [2].

AI.2 Estructura de los Subsistemas de SI

Cada uno de los Subsistemas de SI contiene una serie de requerimientos individuales a cumplir basados en controles, protocolos, reglas, procesos, metodologías y guías de SI. Estos requerimientos son la pieza fundamental del MRU ya que configuran una directiva única e individual, siendo el nivel mínimo de los lineamientos de SI del MRU. Tomemos por ejemplo el requerimiento LS1.2.1 [2] detallado a continuación.}

Requerimiento LS1.2.1
Se deberá elaborar una PSI (Política de SI), cuyo alcance deberá corresponder al definido por la organización en el requerimiento LS1.1.4. La PSI deberá ser de aplicación obligatoria para todo el personal de la organización. *Se recomienda que la misma no supere las 10 carillas, ya que se perderá el entusiasmo de cualquier lector ejecutivo.*

Ilustración AI.2.1: requerimiento LS1.2.1 del MRU [2].

Gracias a la ilustración AI.2.1 podemos comprender fácilmente el propósito de los requerimientos de Seguridad del MRU. Estos se concentran principalmente en detallar un lineamiento individual de seguridad y pretenden ser específicos, para así poder ser referenciados a su vez por otros requerimientos de estadios de madurez superiores. De esta forma, el MRU logra detallar los pasos a seguir para alcanzar, mediante la evolución de niveles de madurez, la mejora continua en SI.

Para facilitar su comprensión por parte del lector, los requerimientos han sido clasificados en función de una taxonomía especial delineada por el MRU. De esta forma, los 9 Subsistemas de SI se dividirán respectivamente en Dominios de Seguridad para así facilitar la organización de los contenidos de cada Subsistema. La gran mayoría de los Subsistemas contendrán un número de dos Dominios llegando a aumentar levemente dicha cantidad en casos excepcionales, para así facilitar el logro del objetivo de simplificar la lectura por parte del profesional de SI.

Tomando como ejemplo el Subsistema de *Gobierno de SI* [2], desarrollado durante el TFE, podrá visualizarse fácilmente (favor de referirse a la ilustración AI.2.2) los dos Dominios de SI que conforman dicho Subsistema: *Enfoque de gobierno de SI* (GOB1) [2] y *Componentes de gobierno de SI* (GOB2) [2].

GOB	Gobierno de SI
GOB1	Enfoque de gobierno de SI
GOB2	Componentes de gobierno de SI

Ilustración AI.2.2: Dominios de Seguridad del Subsistema de Gobierno de Seguridad de la Información del MRU [2].

Luego de la división realizada en diferentes Dominios de Seguridad, el MRU realiza una última clasificación del contenido de los Subsistemas en Áreas de Seguridad. De esta forma, por ejemplo, dentro del Domino de Seguridad GOB2 (Componentes de gobierno

de SI) encontraremos las Áreas de Seguridad *Estrategia de SI* (GOB2.1) y *Distribución de valor para las partes interesadas* (GOB2.2) [2] tal como puede observarse en la ilustración AI.2.3. Dentro de cada una de las Áreas de Seguridad se detallan los requerimientos individuales de cada uno de los Subsistemas del MRU.

GOB	Gobierno de SI
GOB1	Enfoque de gobierno de SI
GOB2	Componentes de gobierno de SI
GOB.2.1	Estrategia de SI
GOB2.2	Distribución de valor para las partes interesadas

Ilustración AI.2.3: Dominios y Áreas de Seguridad del Subsistema de Gobierno de Seguridad de la Información del MRU [2].

De esta forma, el lector fácilmente logrará encontrar en un único lugar todos los requerimientos relativos al Área de Seguridad de interés, sin importar a que estadio de madurez se encuentren vinculados. Cada profesional de seguridad podrá visualizar de forma simple todos los requerimientos desde el estadio mínimo de madurez "E" hasta el nivel de mejora continua "A" y, de esta forma, dilucidar que requerimientos encuentra o no convenientes a través de la selección del estadio de madurez objetivo para su organización.

Se incluye a continuación un esquema que facilitará la descripción de la taxonomía empelada por el MRU para la clasificación de sus requerimientos de SI. Las distintas Áreas y Dominios de SI agrupan y categorizan a los diversos requerimientos del MRU de la siguiente forma:

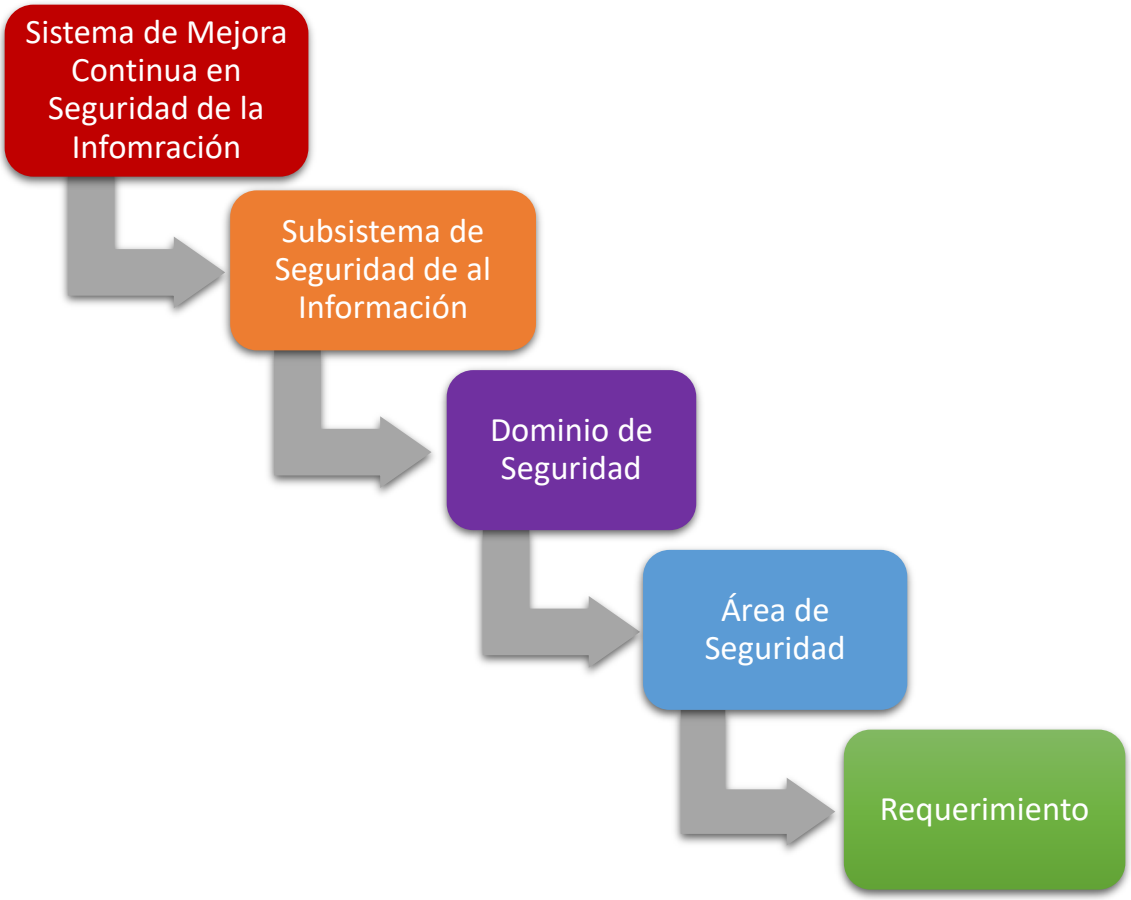

Ilustración AI.2.4: clasificación y organización de requerimientos del MRU.

GOB	Gobierno de SI
GOB.A	Dominio de SI A
GOB.A.1	Área de SI 1
GOB.A.2	Área de SI 2
GOB.B	Dominio de SI B
GOB.B.1	Área de SI 1
GOB.B.2	Área de SI 2

Ilustración AI.2.5: esquema modelo de clasificación de requerimientos.

AI.3 Clasificación de requerimientos de SI

El MRU establece tres tipos diferentes de requerimientos de SI. Dicha clasificación se enfoca principalmente en que el profesional de seguridad pueda diferenciar los requerimientos obligatorios que su organización debe cumplir a la hora de declarar la conformidad con un estadio de madurez específico del MRU. De esta forma, el lector podrá fácilmente diferenciar aquellos requerimientos que el autor considera más importantes para así poder priorizarlos a la hora de su implementación.

"*Cada uno de los requerimientos individuales de SI podrá ser fundamental, clave o especial. Por lo que, dentro del MRU encontraremos tres tipos de requerimientos diferentes:*" [2]

- Fundamentales (F): "*requerimientos obligatorios para declarar conformidad con un cierto nivel MRU. Conformado por todos los requerimientos base de cada estadio de madurez. Corresponde a la gran mayoría de los requerimientos del MRU*" [2].
- Claves (K): "*aquellos requerimientos necesarios para declarar conformidad con un cierto nivel intermedio*[41] *MRU. Corresponden a aquellos requerimientos del nivel inmediatamente superior al que se encuentra la organización que no podrán ser dejados de lado para lograr alcanzar un nivel intermedio MRU*" [2].
- Especiales (S): "*a diferencia de la norma ISO 27.001, que plantea controles genéricos aplicables a cualquier tipo de organización*" [2] "*independientemente de su tipo, tamaño o naturaleza*"[42] [1], "*ciertos requerimientos del MRU no son genéricos y pueden constituir medidas extremadamente excesivas y agresivas para la naturaleza del negocio de determinadas organizaciones. Por este motivo, dichos requerimientos serán considerados como extras para el común de las organizaciones y, solo serán*

[41] Los niveles intermedios implementan parcialmente los requerimientos del nivel MRU inmediatamente superior, realizando énfasis en aquellos requerimientos considerados más importantes. Favor de referirse al capítulo 4 del Trabajo Final de Especialización, para obtener mayor detalle sobre el tema.
[42] En función de lo establecido en la sección 1, página 8 de la Norma IRAM-ISO/IEC 27.001:2015 [1].

necesarios para declarar conformidad para aquellas áreas o sectores críticos a los cuales no todas las organizaciones se encuentran vinculadas:" [2]

a. "*Investigación y desarrollo*" [2].
b. "*Organizaciones contratistas de sectores sensibles de gobiernos*" [2].
c. "*Sectores vinculados al resguardo de la composición, estructura y/o detalle de productos únicos y originales no patentados*" [2].
d. "*Áreas vinculadas a los sectores de defensa y seguridad*" [2].
e. "*Cualquier organización categorizada como una infraestructura crítica en función de la Directiva 2008/114/CE del Consejo de la Unión Europea [3]*" [2].

"*Dichas áreas críticas serán denominadas por el* MRU *como Áreas de Extrema Seguridad (AES), por lo que serán objeto de requerimientos de seguridad especiales*" [2].

AI.4 Formato y estructura de los requerimientos del MRU

En función de la taxonomía detallada anteriormente, el MRU se encontrará dividido en un primer nivel por los 9 Subsistemas de SI. Luego, se procederá a establecer cada uno de los Dominios y Áreas de seguridad correspondientes a cada subsistema, para finalizar detallando cada uno de los requerimientos individuales que conforman el presente marco de referencia.

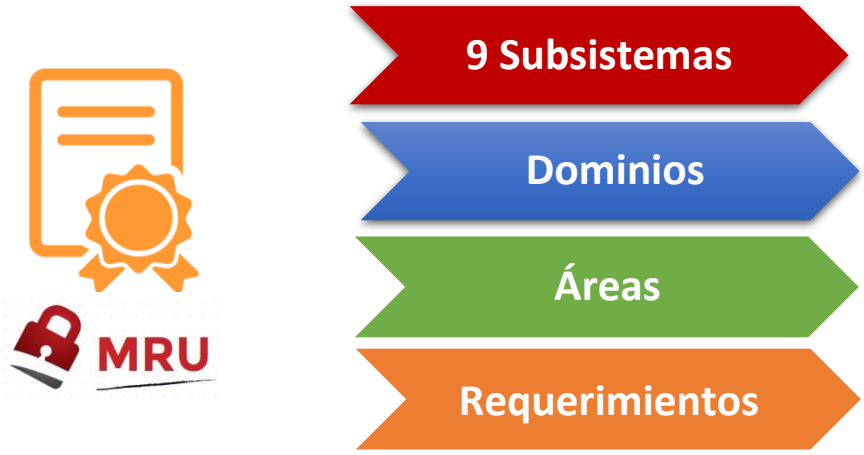

Ilustración AI.4.1: Subsistemas, Áreas y Dominios de SI del MRU [2] [24].

Se incluirá a continuación un ejemplo modelo del formato y estructura de los requerimientos del MRU, con el objetivo de simplificar y facilitar la comprensión por parte del lector. Todos los requerimientos que conforman el MRU se detallarán en el presente trabajo de la siguiente forma:

1. "*Como primer paso se detallará su código univoco, el estadio de madurez MRU al cual corresponde y el tipo de requerimiento (que podrá ser clave, fundamental o especial)*" [2].
2. "*Luego, se procederá a detallar los procesos de los cuales forma parte dicho requerimiento. Esta sección del requerimiento será fundamental para el profesional de seguridad a la hora de construir los mapas de Macroprocesos de seguridad correspondientes a su organización. Se debe tener en cuenta que el requerimiento podría ser parte tanto como de un Macroproceso como a su vez de un subproceso*" [2].
3. "*En tercer lugar se incluirá la descripción del requerimiento en sí*" [2].
4. "*A continuación, se detallarán otros requerimientos del MRU que se encuentran asociados o vinculados de alguna forma a este*" [2].

5. "*Por último, se definirá la documentación fuente*[43] *sobre la cual se basa dicho requerimiento. La documentación fuente hace referencia a todos los marcos de referencia, normas, estándares y guías internacionales y nacionales tomadas como base para la elaboración del presente trabajo*" [2].

Se podrá visualizar fácilmente lo descripto anteriormente en la ilustración que se incluye a continuación. La cual detalla un ejemplo modelo de la estructura de los requerimientos del MRU.

[Código univoco]	[Estadio de madurez]	[Tipo de requerimiento]
[Proceso MRU asociado]		
[Descripción del Requerimiento de seguridad]		
[Requerimientos MRU asociados]		
[Documentación fuente asociada]		

Ilustración AI.4.2: ejemplo modelo de un requerimiento del MRU [2].

Cada uno de los Subsistemas de SI contará con una página que hará las veces de caratula e introducción de este. Dicha página contará con una descripción general del propósito del subsistema y a su vez, detallará la composición de sus respectivos Dominios y Áreas de SI. Favor de referirse a la página 104 del TFE para poder visualizar un ejemplo de dicha sección introductoria [2]. Luego, el MRU procederá a detallar los requerimientos de la primer Área de Seguridad del Subsistema. El ordenamiento de los requerimientos se encuentra basado en el Modelo de Madurez del MRU, por lo que se incluirán en primera instancia los requerimientos asociados a los niveles de madurez inferiores (nivel "E"). Al finalizar cada estadio de madurez, se comienza a detallar todos los requerimientos del nivel inmediatamente superior. De esta forma, el lector puede fácilmente esbozar la

[43] Corresponde a todos los marcos de referencia y normas de seguridad consideradas por el MRU.

evolución de los diferentes lineamientos y exigencias que el MRU establece para una cierta Área de SI, en función del Modelo de Madurez de SI.

A continuación, se incluirá a su vez el requerimiento LS1.1.1 del Subsistema *Lineamientos de Seguridad* (ilustración AI.4.3) con el objetivo de que el lector finalice su proceso de comprensión de la organización y estructura del presente TFM.

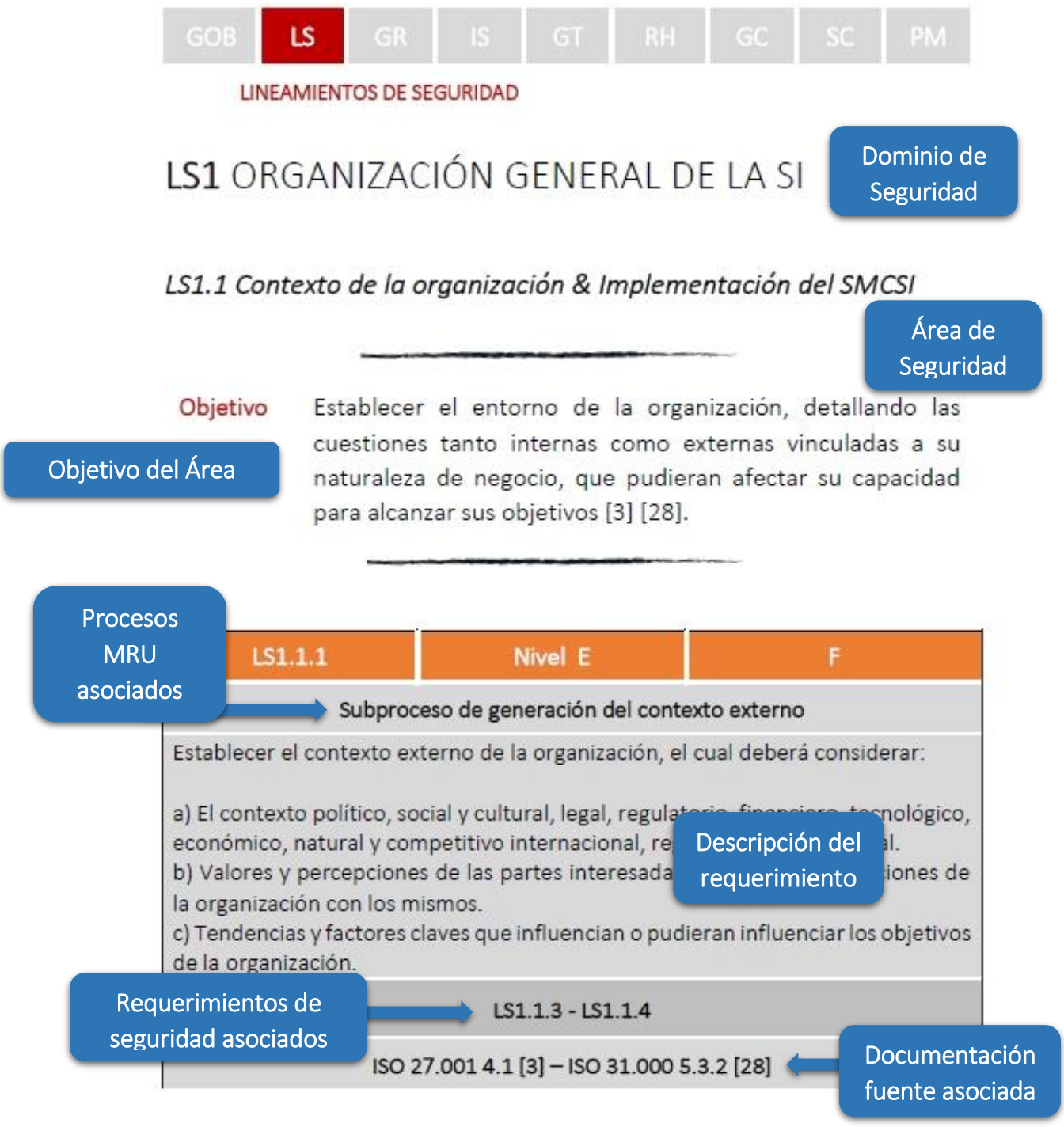

Ilustración AI.4.3: detalle de las secciones del Dominio LS1 del MRU [2].

AI.5 Sobre la construcción de los requerimientos del MRU

Debe tenerse especial atención a que el texto por el cual se encuentra construida la descripción de todos los requerimientos de SI del MRU se basa enteramente en fuentes externad de terceros, los cuales se encuentran adecuadamente referenciados en el borde inferior del requerimiento (sección documentación fuente asociada). En ocasiones, el texto puede diferir del original debido a que:

- Se ha realizado una traducción del texto original en inglés.
- Se ha combinado una o más secciones de diversos documentos que componen la documentación fuente.
- Se han adicionado lineamientos de creación propia (los cuales representan un porcentaje ínfimo del total de requerimientos del MRU).

Lo importante aquí, consiste en detallar que el MRU no conforma un invento puro y exclusivo propio de este autor sino una colección de buenas prácticas clasificadas en función del Modelo de Madurez de SI.

AI.6 Subsistemas de SI faltantes

A continuación, se comenzará a detallar los 7 Subsistemas restantes del MRU, con el objetivo de complementar a los Subsistemas piloto incluidos en el TFE ("*Gobierno de SI*" y "*Lineamientos de Seguridad*" [2]). Recordemos que dichos Subsistemas forman parte del Sistema de Mejora Continua en SI, que el MRU pretende desarrollar.

GR	Gestión de Riesgos
GR1	**Enfoque de Gestión de Riesgos**
GR1.1	Lineamientos de Gestión de Riesgos
GR1.2	Marco de Referencia de Gestión de Riesgos
GR2	**Proceso de gestión de riesgos de SI**
GR2.1	Lineamientos del proceso de gestión de riesgos
GR2.2	Evaluación de riesgos
GR2.3	Tratamiento de riesgos
GR2.4	Monitoreo y mejora continua

IS	Ingeniería de SI
IS1	**Controles Generales de SI**
IS1.1	Seguridad Física y Ambiental
IS1.2	Uso de Activos de Información
IS1.3	Gestión de Accesos
IS2	**Protección y Defensa de la SI**
IS2.1	Protección de la Información
IS2.2	Gestión de incidentes de SI

GT	Gestión de la Tecnología
GT1	Seguridad de los sistemas y la tecnología
GT1.1	Tecnología de SI
GT1.2	Gestión de sistemas de información
GT2	Gestión de la Tecnología de la Información
GT2.1	Lineamientos de Gestión y Eficiencia Operativa

RH	Gestión de los Recursos Humanos
RH1	Gestión de la Seguridad de los Recursos Humanos
RH1.1	"*Antes del empleo*" [1]
RH1.2	"*Durante el empleo*" [1]
RH1.3	"*Después del empleo*" [1]
RH2	Programa de Toma de Conciencia, Entrenamiento y Difusión
RH2.1	Metodología de Conciencia, Entrenamiento y Difusión

GC	Gestión de la Continuidad
GC1	Continuidad de la SI
GC1.1	Lineamientos & Sistema de Continuidad

SC	Seguimiento y Control de la SI
SC1	Revisión Gerencial de la SI
SC1.1	Evaluación y Monitoreo de la SI
SC1.2	No conformidades y acciones correctivas
SC2	Auditoria de la SI
SC2.1	Lineamientos de Auditoria de SI

PM	Procesos y Mejora Continua de la Seguridad
PM1	Procesos de SI
PM1.1	Lineamientos de la gestión de seguridad orientada a procesos
PM2	Mejora Continua de SI
PM2.1	Programa de mejora continua & compliance de SI

Ilustración AI.6.1: guía de detalle de los Subsistemas faltantes del MRU.

[Página dejada en blanco intencionalmente]

GESTIÓN DE RIESGOS

El objetivo primordial del presente subsistema comprende el establecimiento de los lineamientos principales del corazón de la Seguridad de la Información: la gestión de riesgos.

Se enfoca principalmente en la una metodología especifica de gestión de riesgos integral, holística y a medida de la organización, realizando énfasis en aquellas actividades, procesos y aplicaciones críticas del negocio. Dicha metodología conformará la base del proceso de gestión de riesgos establecido por el MRU en función de los lineamientos del ISF, ISO y COBIT [1] [4] [5] [6].

GR1 Enfoque de gestión de riesgos

GR1.1 Lineamientos de gestión de riesgos

GR1.2 Marco de referencia de gestión de riesgos

GR2 Proceso de gestión de riesgos de Seguridad de la Información

GR2.1 Lineamientos del proceso de gestión de riesgos

GR2.2 Evaluación de riesgos

GR2.3 Tratamiento de riesgos

GR2.4 Monitoreo y mejora continua

GR1 ENFOQUE GESTIÓN DE RIESGOS

GR1.1 Lineamientos de Gestión de Riesgos

Objetivo Establecer los fundamentos de la gestión del riesgo de Seguridad de la Información para así facilitar la integración del esquema de gobierno de la organización con el proceso de gestión de riesgos en función de los lineamientos delineados por COBIT, ISO, OCDE e ISF [1] [4] [5] [6].

GR1.1.1	Nivel D	F
Macroproceso de gestión de riesgos de SI		
La alta dirección de la organización será responsable de la aprobación de la metodología de gestión de riesgos de SI aplicada por la organización (la cual estará establecida dentro del proceso de gestión de riesgos de SI) y de sus subsecuentes actualizaciones y modificaciones. La misma deberá: a) Brindar su total apoyo para el desarrollo del proceso y su mantenimiento en el tiempo. b) Basarse en enfoque de ataque sistémico a los riesgos de SI. c) Encontrarse alineada con la gestión global de riesgo de la organización. d) Integrar a la gestión del riesgo como una parte integral de todas las actividades de SI. e) Aplicarse tanto durante el diseño como durante la ejecución del Sistema de Mejora Continua en SI. f) Bajarse a tierra como un proceso de ejecución continua en el tiempo.		

La gestión de riesgos de SI debe de ser consistente e integrada con la gestión de riesgos de la organización para así resultar en una armonización de los requerimientos del negocio y de SI. Si la organización ya tuviera en funcionamiento una metodología de gestión de riesgos deberá adaptar la misma a los requerimientos del presente Subsistema.

El RMO junto con los RRs, serán responsables de la ejecución del proceso de gestión de riesgos de SI.

El RMO será responsable del diseño del proceso de gestión de riesgos de SI de la organización, el cual deberá incorporar todos los lineamientos del presente Subsistema de seguridad.

El CISO debe diseñar, establecer, dirigir, monitorear, mejorar y comunicar un Marco de referencia de gestión de riesgos de SI de la organización (referirse a GR1.2).

El CISO será responsable del desarrollo, implementación y mantenimiento del plan global de gestión de riesgos de SI de la organización (referirse a GR1.2.7). La dirección ejecutiva, o el CSI para estadios "C" y superiores, deberá aprobar dicho plan.

GR1.2 – GR1.2.7
ISO 27.001 6.1.2 y 6.1.3 [3] – ISO 31.000 Introducción – ISO 27.005 5 [11]

GR1.1.2	Nivel D	F
Proceso de gestión de riesgos de SI		

El proceso de gestión de riesgos de SI deberá realizarse periódicamente según un plazo establecido por la organización, siempre y cuando durante ese lapso no se modifique:

a) La infraestructura y/o arquitectura de TI de la organización.
b) Los procesos de negocio de la organización.
c) Los objetivos generales estratégicos de la organización.
d) Los requerimientos legales, reglamentarios, estatutarios y contractuales aplicables a la organización.

El lapso entre ejecuciones establecido por la organización no deberá ser mayor a los 12 meses.

ISO 27.001 6.1.2.b y 8.2 [1]

GR1.1.3	Nivel D	F

Proceso de gestión de riesgos de SI

La organización deberá de definir su apetito de riesgo. El apetito deberá encontrarse definido en función de:

a) Los criterios de aceptación del riesgo de SI.
b) Los criterios para la realización de la evaluación del riesgo de SI.
c) Riesgos de incumplimiento de requerimientos legales, regulatorios, reglamentarios, estatutarios, de mercado, entre otros.
d) Disrupciones en las operaciones de la organización.
e) Daño reputacional.
f) Pérdida de valor.
g) Pérdidas financieras o económicas.
h) Pérdida de ventaja competitiva.
i) Riesgos de responsabilidad civil.

El apetito de riesgo deberá ser comunicado y entendido por todos aquellos en la organización que tomen decisiones sobre el tratamiento de riesgos.

Se recomienda la utilización de alguna técnica estructurada.

Si las unidades de negocio poseen una independencia marcada o la estructura de la organización es extensa e inconsistente, se recomienda que el apetito de riesgo sea definido a nivel de unidades de negocio.

El apetito de riesgo conforma los llamados "criterios de aceptación del riesgo" definidos por la ISO 27.001 6.1.2.a.1 [1].

ISF parte introductoria, SG2.3.1 y SG2.3.2 [4] – ISO 27.014 5.2.2 [7]

- ISO 27.001 6.1.2.a [1] –

GR1.1.4	Nivel D	F
El apetito de riesgo puede estará sujeto a cambios frecuentes como resultado de: a) Cambios de la estrategia de negocio de la organización. b) Cambios en las expectativas de las partes interesadas. c) Fusiones, adquisiciones o crecimiento de la organización. e) Dificultades económicas. f) Aumento de la competencia. g) Evolución de las amenazas a los activos de información. h) La ocurrencia de incidentes importantes de SI. i) Desarrollo de nuevos productos o servicios. La organización deberá actualizar el apetito de riesgo ante la ocurrencia de alguno de los eventos mencionados en el presente requerimiento.		
ISF parte introductoria, SG2.3.1 y SG2.3.2 [4] – ISO 27.014 5.2.2 [7] - ISO 27.001 6.1.2.a [1] –		

GR1.1.5	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá conservar información documentada sobre el diseño, implementación, ejecución, revisión y mejora del proceso de gestión de riesgos de SI.		
ISO 27.001 6.1.2 y 8.2 [1]		

GR1.1.6	Nivel D	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos debe estar alineado con la cultura, procesos, estructura y estrategia de la organización. El contexto definido en LS1.1.1 y LS1.1.2 y las partes interesadas identificadas en LS1.1.3 serán utilizados como input para el proceso de gestión de riesgos. La gestión de riesgos debe: a) Estar coordinada como un programa holístico de toda la organización. b) Estar basada en la evaluación de riesgos de información que puedan comprometer el logro de los objetivos de la organización. c) Tomar como punto de entrada los resultados de la aplicación de los requerimientos LS1.1.1, LS1.1.2 y LS1.1.3. d) Poseer un alcance idéntico al establecido en LS1.1.4. e) Identificar, evaluar, priorizar, tratar y monitorear los riesgos de SI. f) Involucrar a las partes interesadas en las decisiones de gestión de riesgos. g) Tomar el contexto de la organización (LS1.1.1 y LS1.1.2). *Se recomienda que se evalúe aplicar d) con un alcance que tienda a alcanzar a toda la organización a fines de facilitar la adopción de requerimientos con niveles de madurez superiores.*		
LS1.1.1 - LS1.1.2 - LS1.1.3 – GR1.1.1		
ISO 27.001 6.1.2 y 8.2 [1] – [4] – [5] – ISO 27.005 5 y 6 [11]		

GR1.1.7	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá establecer una política de gestión de riesgos. La misma debe detallar: a) Los objetivos de la organización vinculados a la gestión de riesgos. b) El compromiso de la organización de gestionar sus riesgos. c) Responsabilidades y autoridades de gestión de riesgos.		

d) La forma en la que la organización resolverá los conflictos de interés.
e) La conformación del EGR de la organización. A su vez deberá detallar sus funciones, autoridades y responsabilidades en función de LS2.2.1.
f) El compromiso de la organización con la revisión y mejora continua tanto de la política riesgos como del marco de referencia de gestión de riesgos.

La política de gestión de riesgos deberá ser comunicada a todas las partes interesadas de la organización.

En función de b) la organización deberá manifestar su compromiso de asignación de los recursos necesarios a las autoridades de gestión de riesgos mencionadas en c) y e).

La organización debe comprometerse a implementar f) en forma periódica y ante cualquier evento o cambio mencionado en GR1.1.4.

c) hace referencia al personal de la organización que deberá tener no solo la responsabilidad sino la autoridad para realizar la gestión de riesgos de SI.

LS2.2.1
ISO 31.000 4.3.2 [6]

GR1.1.8	Nivel E	F
Proceso de gestión de riesgos de SI		

La organización deberá regirse por los siguientes principios de gestión de riesgos:

a) **La gestión de riesgos debe crear valor y protegerlo**. La gestión de riesgos debe contribuir a alcanzar los objetivos estratégicos de la organización y no a dificultar o entorpecer las acciones delineadas para alcanzarlos.
b) **La gestión de riesgos deberá formar parte e integrarse con la toma de decisiones dentro de la organización**. La gestión de riesgos colabora a los decisores a tomar daciones informadas, a priorizar sus opciones y acciones y a distinguir entre diversas alternativas de acción y sus posibles impactos en el logro de los objetivos estratégicos de la organización.
c) **La gestión de riesgos debe explícitamente abordar la incertidumbre**. Deberá tomarla en cuenta, clasificarla, documentarla y delinear alternativas para su tratamiento.

d) **La gestión de riesgos debe ser sistemática y estructurada**. De esta forma, logrará ser consistente en el tiempo permitiendo así la producción de resultados confiables y comprables en el tiempo.
e) **La gestión de riesgos debe basarse en la mejor información disponible**. No siempre se contará con toda la información necesaria o completa (datos históricos, experiencia, recomendaciones de expertos, pronósticos, entre otros) a la hora de tomar decisiones de riesgos. Por este motivo, los decisores deberán informarse y tomar en cuenta cualquier tipo de limitación de datos o del modelo utilizado que pueda ocasionar divergencias de opinión ante qué alternativas de decisión se deben encarar.

Dichos principios deberán encontrarse documentados e integrados con la política de gestión de riesgos de la organización (GR1.1.7).

GR1.1.7
ISO 31.000 3 [6]

GR1.1.9	Nivel C	F
Proceso de gestión de riesgos de SI		
El CSI será el responsable estratégico de la gestión de riesgos de SI de la organización. Será responsable de la aprobación de la metodología de gestión de riesgos de SI aplicada por la organización (la cual estará establecida dentro del proceso de gestión de riesgos de SI) y de sus subsecuentes actualizaciones y modificaciones. El mismo deberá brindar su total apoyo para el desarrollo del proceso y su mantenimiento en el tiempo. El RMO y el CIPO serán responsables del desarrollo e implementación de mejoras al proceso de gestión de riesgos de SI de la organización. Dichas mejoras serán presentadas al CSI para su aprobación. El órgano rector de gobierno de la organización debe diseñar, establecer, dirigir, monitorear, mejorar y comunicar un Marco de referencia de gestión de riesgos de SI de la organización (referirse a GR1.2). *Cabe resaltar que la responsabilidad del Marco de referencia de gestión de riesgos de SI de la organización ha pasado a manos del órgano rector de gobierno de la*		

organización a diferencia de lo establecido en GR1.1.1 como nivel de madurez inferior.

GR1.1.10	Nivel C	K
Proceso de gestión de riesgos de SI		
La organización deberá de establecer una política de gestión de riesgos. Dicha política deberá detallar: a) La razón fundamental por la que la organización decide gestionar sus riesgos. b) Los vínculos de los objetivos y las políticas de la organización con la política de gestión de riesgos. c) La forma en la que la performance de la gestión de riesgos será medida y reportada al CEP, al CSI y al órgano rector de gobierno de la organización.		
ISO 31.000 4.3.2 [6]		

GR1.1.11	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá regirse por los siguientes principios de gestión de riesgos: a) **La gestión de riesgos debe ser a medida de la organización**. Deberá estar alineada perfectamente al contexto interno y externo y, a su vez, al apetito de riesgo establecido por la organización. b) **Se debe respetar el gobierno de riesgos, los lineamientos para la gestión de riesgos y principalmente los tiempos establecidos para su ejecución.** La organización deberá asegurarse de haber asignado la autoridad, entrenamiento, recursos, capacidades y tiempo suficiente a fin de que aquellos que ocuparan roles de gestión de riesgos de SI puedan asumir sus responsabilidades plenamente. c) **La gestión de riesgos debe ser dinámica, iterativa y adaptable a cambios**. Se debe mejorar continuamente la gestión de riesgos de la organización debido a que el contexto (tanto interno como externo) variará continuamente en el tiempo,		

surgirán nuevos riesgos que no fueron tomados en cuenta y, a su vez, riesgos considerados y tratados podrán desaparecer. Dichos principios deberán encontrarse documentados e integrados con la política de gestión de riesgos de la organización (GR1.1.7).
GR1.1.7
ISO 31.000 3 y Anexo A A.3.2 [6]

GR1.1.12	Nivel C	K
Proceso de gestión de riesgos de SI		
La definición de roles de gestión de riegos de SI (en conjunto con sus respectivas responsabilidades y autoridad), la política y el proceso de gestión de riesgos de SI y el Marco de referencia de gestión de riesgos de SI de la organización deberán formar parte de todos los programas de inducción de la organización. A su vez, la organización deberá realizar capacitaciones regulares sobre las temáticas detalladas en el presente requerimiento. *La implementación del presente requerimiento deberá realizarse dentro del alcance del Programa de toma de Conciencia, Entrenamiento y Difusión de SI del MRU.*		
ISO 31.000 Anexo A A.3.2 [6]		

GR1.1.13	Nivel B	F
Proceso de gestión de riesgos de SI		
La gestión de riesgos debe cubrir a toda la organización, incluyendo sus puntos de contacto e integración con otras organizaciones (por ejemplo: tercerización de servicios, proveedores, clientes, entre otros). *El presente requerimiento restringe la libertad de alcance establecida en GR1.1.6.d debido a que el estadio de madurez B es únicamente compatible con un SMCSI de alcance global a toda la organización.*		

GR1.1.14	Nivel B	F
Proceso de gestión de riesgos de SI		
La organización deberá regirse por los siguientes principios de gestión de riesgos: a) **La gestión de riesgos debe ser transparente e inclusiva**. Se debe involucrar a las partes interesadas en tiempo y forma y, en particular, a todos aquellos tomadores de decisión de todos los niveles de la organización dentro de la gestión de riesgos. El involucramiento permite que la organización pueda tomar en cuenta todos los puntos de vista para así lograr que las partes interesadas sean apropiadamente representadas a la hora de gestionar riesgos. b) **La gestión de riesgos debe ser una parte integral de todos los procesos de la organización**. La gestión de riesgos no debe ser una actividad no integrada con el negocio. Debe de integrarse con las actividades y procesos de la organización y, a su vez, ser una responsabilidad de la dirección ejecutiva. c) **La gestión de riesgos deberá considerar los factores culturales y humanos**. La gestión de riesgos debe reconocer que las capacidades, percepciones e intenciones de personas (tanto internas como externas a la organización) podrán tanto facilitar como obstaculizar el logro de los objetivos estratégicos de la organización. Dichos principios deberán encontrarse documentados e integrados con la política de gestión de riesgos de la organización (GR1.1.7).		
GR1.1.7		
ISO 31.000 3 [6]		

GR1.1.15	Nivel B	F
Proceso de gestión de riesgos de SI		
El CEP y el CIPO serán responsables del desarrollo e implementación de mejoras al proceso de gestión de riesgos de SI de la organización. Dichas mejoras serán presentadas al CSI para su aprobación.		

El RMO será responsable del diseño del proceso de gestión de riesgos de SI de la organización, el cual deberá incorporar todos los lineamientos del presente Subsistema de seguridad.

Cabe resaltar que la responsabilidad del proceso de gestión de riesgos de SI de la organización ha pasado a manos del CEP a diferencia de lo establecido en GR1.1.1 como nivel de madurez inferior.

GR1.1.9 – GR1.1.1
ISO 31.000 3 [6]

GR1.1.16	Nivel B	F
Proceso de gestión de riesgos de SI		
Toda toma de decisión vinculada a la SI, sin importar su nivel de importancia, deberá haber involucrado la consideración explicita de riesgos de SI y la aplicación de la gestión de riesgos de SI hasta un cierto grado apropiado para el nivel de importancia de dicha decisión. La aplicación del presente requerimiento podrá reflejarse en los registros de reuniones y decisiones que documenten que se han realizado discusiones, debates o análisis explícitos de riesgos de SI.		
ISO 31.000 Anexo A A.3.3 [6]		

GR1.1.17	Nivel A	F
Proceso de gestión de riesgos de SI		
La organización deberá de regirse por los siguientes principios de gestión de riesgos: a) **La gestión de riesgos debe facilitar la mejora continua de la organización**. Se deberán implementar estrategias tendientes a mejorar la madurez de la gestión de riesgos en forma conjunta con otros aspectos tanto de seguridad como de gestión de la organización.		

Dichos principios deberán encontrarse documentados e integrados con la política de gestión de riesgos de la organización (GR1.1.7).
GR1.1.7
ISO 31.000 3 [6]

GR1 ENFOQUE GESTIÓN DE RIESGOS

GR1.2 Marco de referencia de Gestión de Riesgos

Objetivo Establecer el marco de referencia de la gestión del riesgo de Seguridad de la Información, el cual logrará establecer el marco de acción a la gestión a la hora de implementar la gestión de riesgos de seguridad de la organización. De esta forma se podrá lograr un perfecto alineamiento a los objetivos estratégicos del negocio.

GR1.2.1	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización debe asegurarse de establecer tanto la responsabilidad como la autoridad para la gestión de riesgos a responsables competentes e idóneos dentro o fuera de la organización. Para lo cual, la organización deberá diseñar, implementar y mantener un Marco de Referencia de Gestión de Riesgos. El mismo deberá contemplar: a) La identificación de los RRs (Responsables de riesgos individuales), que tendrán responsabilidad y autoridad para gestionar los respectivos riesgos que les han sido asignados. b) El establecimiento de un RMO (referirse a LS2.1.8), quien será responsable de llevar a delante la gestión de riesgos de SI de la organización.		

c) La identificación y el establecimiento de otras responsabilidades del personal de la organización para el diseño, implementación, ejecución y mejora del proceso de gestión de riesgos.
d) El diseño, establecimiento y mejora de los mecanismos (procesos, políticas, procedimientos, etc.) necesarios para la implementación de los requerimientos de GR1.
e) Sus 2 componentes fundamentales detallados en GR1.2.2.

A los fines de este requerimiento, la gestión de riesgos de SI comprende el diseño, implementación, ejecución y el mantenimiento del proceso de gestión de riesgos de SI, como así también la efectividad, suficiencia, diseño, implementación y mejora de los controles que resulten del mismo.

Se recomienda que los RRs sean seleccionados en función de su conocimiento del negocio. La selección de estas autoridades de seguridad e la información no debe circunscribirse únicamente al personal de las áreas de riesgos, seguridad o TI, sino que debe enfocarse en aquellos tomadores de decisión dentro del negocio.

ISO 31.000 4.3.3 y 4.1 [6]

GR1.2.2	Nivel D	F

Proceso de gestión de riesgos de SI

El Marco de Referencia de Gestión de Riesgos de SI deberá contener 2 componentes fundamentales:

a) Diseño del Marco de Referencia de Gestión de Riesgos de SI.
   I. *Entendimiento de la organización y su contexto: GR1.1.6.*
   II. *Establecimiento de una política de gestión de riesgos: GR1.1.7.*
   III. *Responsabilidad y autoridad: GR1.1.1, GR1.1.3, GR1.1.5 y GR1.1.6.*
   IV. *Recursos: GR1.1.4.*
b) Implementación de la gestión de riesgos de SI.
   I. *Implementación del marco de referencia de gestión de riesgos de SI: GR1.2.8.*
   II. *Implementación del proceso de gestión de riesgos de SI: GR1.2.7.*

La organización posee total libertad para el diseño de los componentes de su Marco de Referencia de Gestión de Riesgos de SI. Por lo que es libre de adicionar, fusionar o combinar los componentes del presente requerimiento. No obstante, deberá adaptar, en la forma más conveniente a su naturaleza, los componentes del presente requerimiento.

Se recomienda que la organización tome como base su actual marco de referencia de gestión de riesgos de SI (de existir).

Se debe tener especial atención a GR1.1.6 ya que, el contexto influenciara significativamente el diseño del Marco de Referencia.

ISO 31.000 4.1 [6]

GR1.2.3	Nivel D	F

Proceso de gestión de riesgos de SI

Los RRs (Responsables de riesgos individuales) deberán:

a) Velar por la correcta gestión de los riesgos que les han sido asignados.
b) Ser miembros del EGR y concurrir a sus reuniones cuando los riesgos que les fueren asignados se encuentren bajo análisis.
c) Supervisar el correcto diseño, implementación, mejora y suficiencia de los controles asociados a los riesgos de los cuales es responsable. El EGR será responsable por el diseño y mejora del control, mientras que los RRs, junto al RMO, serán responsables de la implementación.
d) Contar con responsabilidades claramente definidas y con la autoridad total para poder llevar adelante una óptima gestión de los riesgos a su cargo.
e) Tener asignados los recursos necesarios para revisar, monitorear y mejorar controles, para monitorear riesgos y para comunicar efectivamente sobre sus riesgos asignados y su respectiva gestión a las partes interesadas internas y externas.

Los RRs son quienes comprenden el negocio. Es por este motivo que ofrecen un punto de vista fundamental a la hora de gestionar los riesgos asociados a los activos de información de la organización ya que, son quienes trabajan día a día con dichos activos.

Los RRs deberán aceptar las responsabilidades por la gestión de los riesgos que le han sido asignados. Dicha aceptación deberá ser documentada por la organización. A su vez, deberá encontrarse detallada en las descripciones del puesto.
ISO 31.000 4.3.3 y Anexo A.3.2 [6]

GR1.2.4	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá asignar los recursos apropiados para la gestión de riesgos. Dichos recursos comprenden, pero sin limitarse a: a) RRHH, habilidades, experiencia y competencias. b) Recursos necesarios para cada actividad y subproceso del proceso de gestión de riesgos. c) Métodos y técnicas utilizadas para gestionar riesgos. d) Sistemas de gestión del conocimiento y de la información. e) Programas de capacitación y entrenamiento. f) Recursos necesarios para documentar e integrar a la gestión de riesgos los procesos de la organización.		
ISO 31.000 4.3.5 [6]		

GR1.2.5	Nivel D	F
Proceso de gestión de riesgos de SI		
El RMO deberá: a) Ejecutar la política de gestión de riesgos de SI de la organización en función de GR1.1.7. b) Presidir el EGR, organismo encargado de ejecutar la gestión de riesgos de SI según LS2.2.1.		

c) Asegurarse que la política de gestión de riesgos se encuentre actualizada e implementada. d) Buscar la aprobación de la política de gestión de riesgos de SI. e) Implementar los controles vinculados a riesgos de SI, en conjunto con los RRs correspondientes. f) Diseñar, mantener y mejorar el proceso de gestión de riesgos de SI. *El accionar del EGR y el RMO deberá estar enmarcado dentro de los lineamientos establecidos por el Marco de referencia de gestión de riesgos de SI.*
ISO 31.000 4.3.3 y 4.3.4 [6]

GR1.2.6	Nivel D	F
Proceso de gestión de riesgos de SI		
El EGR será responsable de: a) Ejecutar la gestión de riesgos de SI según LS2.2.1, en función de la política de gestión de riesgos de la organización. b) Gestionar los riesgos de SI de la organización a través del proceso de gestión de riesgos establecido al caso. c) Diseñar, monitorear y mejorar los controles vinculados a riesgos de SI. Deberá a su vez analizar si los controles son apropiados y suficientes. d) Supervisar la implementación de los controles mencionados en c). *El accionar del EGR y el RMO estará enmarcado dentro de los lineamientos establecidos por el Marco de referencia de gestión de riesgos de SI.*		
ISO 31.000 4.3.3 [6]		

GR1.2.7	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá asegurarse que el proceso de gestión de riesgos de SI sea implementado a través de un plan global de gestión del riesgo de SI en todos los niveles y áreas funcionales de la organización. *De esta forma se logrará la uniformidad necesaria para que la gestión de riesgos sea estructurada y medible a lo largo del tiempo.*		
ISO 31.000 4.3.4 y 4.4.2 [6]		

GR1.2.8	Nivel D	F
Proceso de gestión de riesgos de SI		
Para lograr una implementación exitosa del Marco de Referencia de gestión de riesgos de SI, la organización debe: a) Definir una estrategia y un cronograma de actividades apropiado para la implementación del Marco de Referencia. b) Aplicar la política de gestión de riesgos de SI y el proceso de gestión de riesgos de SI e integrar los mismos a los procesos de negocio de la organización. c) Identificar, documentar e integrar al Marco de Referencia todos los requerimientos legales, estatutarios, regulatorios y de mercados a los cuales eta sujeta la organización. d) Implementar un programa de capacitación y toma de conciencia de la gestión del riesgo a lo largo de toda la organización, realizando énfasis en aquellos decisores que serán considerados RRs, las autoridades de SI y todo RRHH que estará vinculado a tareas de gestión de riesgos. e) Comunicarse con y consultar a las partes interesadas regularmente para asegurarse que el Marco de Referencia continua siendo actual y apropiado. f) Asegurarse que la toma de decisiones y el desarrollo y establecimiento de objetivos se encuentre alineada con los resultados del proceso de gestión de riesgos de SI. *La organización deberá asegurarse de cumplir con todos los requisitos detallados en c).*		

d) estará integrado dentro del Programa de toma de Conciencia, Entrenamiento y Difusión del MRU.

Se recomienda que la estructura del Marco de Referencia de gestión de riesgos de SI sea diseñada en forma de cascada según puede visualizarse en GR1.2.8.A.

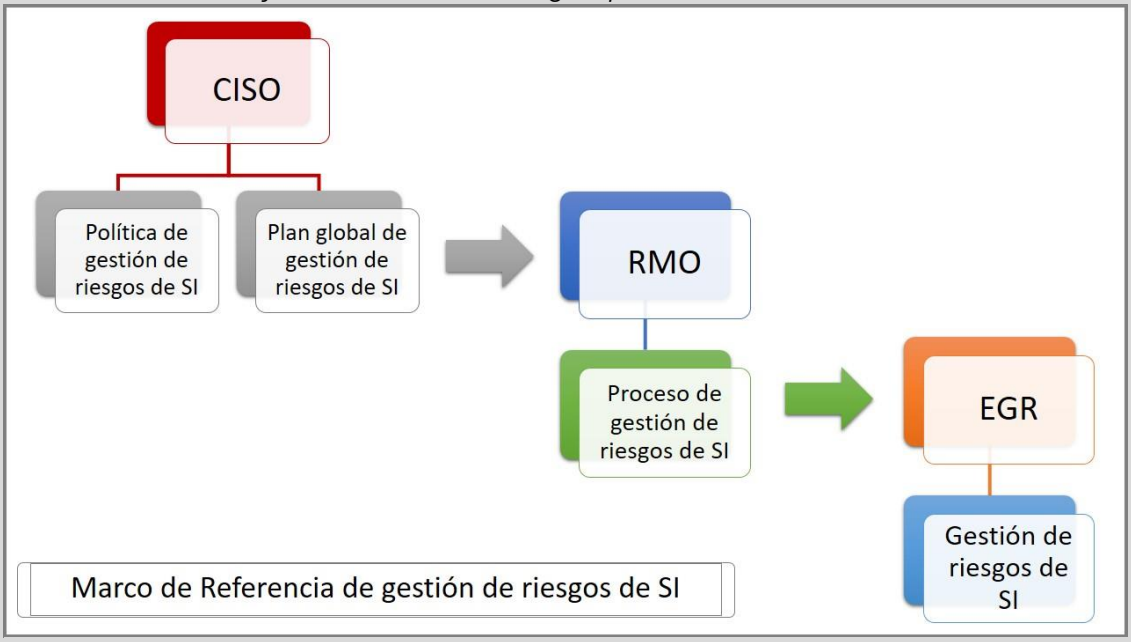

Ilustración GR1.2.10.A: Estructura modelo de gobierno de riesgos de SI.

ISO 31.000 4.3.3 [6]

GR1.2.9	Nivel C	F

Proceso de gestión de riesgos de SI

La organización deberá diseñar un Marco de Referencia de Gobierno de Riesgos de SI en función de lo establecido en GOB1.2.2, GR1.2.1, GR1.2.2 y en el presente requerimiento.

En base a GR1.2.2, el Marco de Referencia de Gobierno de Riesgos de SI deberá contener los siguientes componentes fundamentales:

a) Compromiso y mandato: *GR1.1.12, GR1.1.13 y GR1.1.14.*
b) Diseño Marco de Referencia de Gobierno de Riesgos de SI.

I. *Entendimiento de la organización y su contexto: GR1.1.6.*
II. *Establecimiento de una política de gestión de riesgos: GR1.1.7.*
III. *Responsabilidad y autoridad: GR1.1.1, GR1.1.3, GR1.1.5 y GR1.1.6.*
IV. *Integración con los procesos de la organización: GR1.1.12.*
V. *Recursos: GR1.1.4.*
VI. *Comunicación interna y reporte: GR1.1.17.*
VII. *Comunicación externa y reporte: GR1.1.18.*

c) Implementación de la gestión de riesgos de SI.

I. *Implementación del Marco de Referencia de Gobierno de Riesgos de SI: GR1.2.8.*
II. *Implementación del proceso de gestión de riesgos de SI: GR1.2.7.*

d) Monitoreo y revisión del Marco de Referencia de Gobierno de Riesgos de SI: GR1.1.16.

La organización creará su propio marco de referencia en función de sus necesidades, la naturaleza de su negocio, su estructura organizacional y su cultura. No obstante, deberá adaptar, en la forma más conveniente a su naturaleza, los componentes del presente requerimiento.

Se recomienda que la organización tome como base su actual marco de referencia de gestión de riesgos de SI (de existir).

GR1.2.1 – GR1.2.2 – GOB1.2.2

GR1.2.10	Nivel C	F

Proceso de gestión de riesgos de SI

La organización deberá establecer una estructura de gobierno de riesgos de SI que se adecue a lo establecido en GR1.1.1, GR1.1.9 y GR1.2.9. Dicha estructura deberá a su vez diseñarse en forma de cascada según puede visualizarse en la ilustración GR1.2.10.A.

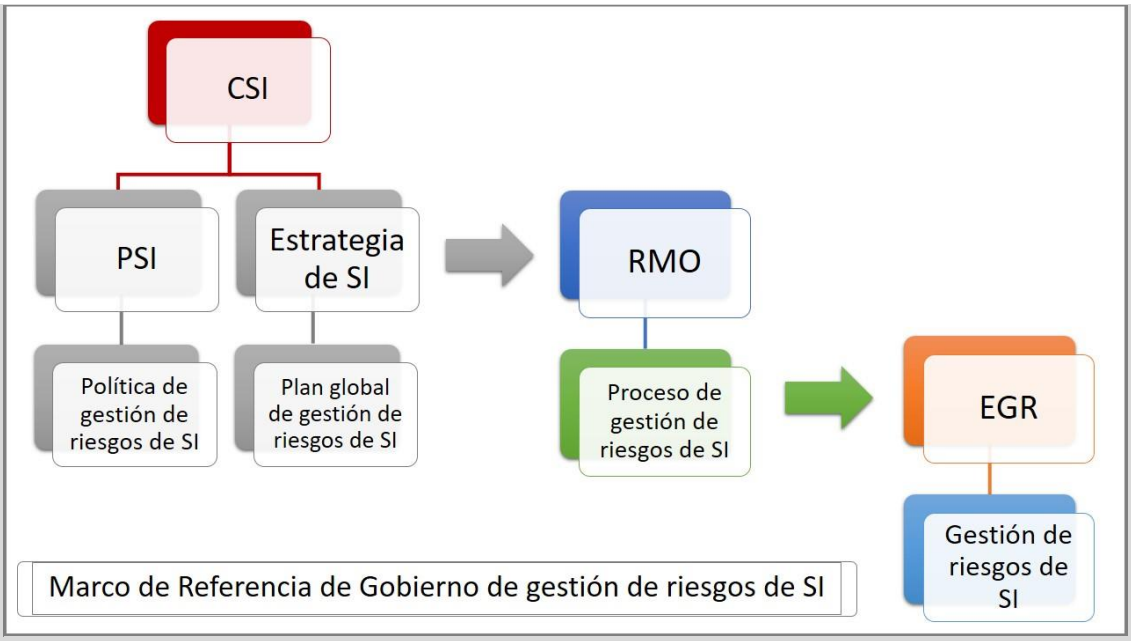

Ilustración GR1.2.10.A: Estructura modelo de gobierno de riesgos de SI.

ISO 31.000 4.3.3 [6]

GR1.2.11	Nivel C	F

Proceso de gestión de riesgos de SI

La organización deberá eestablecer un mecanismo de medición y reporte de la performance de la gestión de riesgos.

Dicho mecanismo deberá:

a) Medir la performance de la gestión de riesgos contra KPIs diseñados y revisados regularmente tanto por el CSI como por el órgano rector de gobierno de la organización.
b) Medir periódicamente el progreso de la gestión de riesgos de SI (y cualquiera de sus desviaciones) con respecto al plan global de gestión de riesgos de SI.
c) Medir el progreso de la implementación de los planes de tratamiento de riesgos de SI.

ISO 31.000 4.3.3, 4.5 y 5.6 [6]

GR1.2.12	Nivel C	F
Proceso de gestión de riesgos de SI		
El Marco de Referencia de gobierno de riesgos de SI deberá de proveer un mecanismo para facilitar la integración de la gestión de riesgos con las prácticas y procesos de la organización en forma eficaz y eficiente. *El proceso de gestión de riesgos debe llegar a convertirse en parte de los procesos de la organización y no conformar un proceso aislado sin integración alguna con los demás de su tipo.* Por lo tanto, en función de GR1.2.7, la organización deberá desarrollar un plan estratégico global de gestión de riesgos de SI, el cual deberá asegurar que: a) La política de gestión de riesgos se encuentre actualizada e implementada. b) La gestión de riesgos se encuentre embebida dentro de las prácticas y los procesos de la organización. c) Que la gestión del riesgo de SI se encuentre embebida dentro del desarrollo de políticas de seguridad y de los procesos de gestión del cambio. d) Los objetivos de gestión de riesgos de SI se encuentren perfectamente alineados con los objetivos y estrategias de la organización. e) El cumplimiento de los requisitos legales, regulatorios, estatutarios y de mercado. *El plan global de gestión del riesgo podrá ser integrado dentro de otros planes organizacionales (tales como el PESI, que el MRU establece en GOB2.1.4).*		
ISO 31.000 4.3.4 y 4.2 [6]		

GR1.2.13	Nivel C	F
Proceso de gestión de riesgos de SI		
El órgano rector de gobierno de la organización deberá: a) Ratificar la política de gestión de riesgos de SI, a través de su firma (luego de haber sido generada por el RMO y, luego, aprobada por el CSI según GR1.2.14).		

b) Asegurarse que los recursos necesarios para el desarrollo de la gestión de riesgos hayan sido adecuadamente asignados. c) Asegurar el compromiso de todos los niveles de la organización para la gestión de riesgos de SI. d) Comunicar los beneficios de la gestión de riesgos de SI a todas las partes interesadas. e) Aprobar el Marco de Referencia de gobierno de riesgos de SI y, a su vez, asegurarse de que el mismo continúe siendo apropiado. f) Asignar las responsabilidades y autoridades necesarias en los diversos niveles de la organización para la correcta implementación y aplicación del presente Subsistema de SI. g) Ser el responsable del diseño, implementación y mejora del marco de referencia de gobierno de riesgos de SI establecido en GR1.2.5.
ISO 31.000 4.2 [6]

GR1.2.14	Nivel C	F
Proceso de gestión de riesgos de SI		
El CSI será responsable de: a) Aprobar la política de gestión de riesgos de SI. b) Asegurarse que la política de gestión de riesgos de SI se en encuentre en concordancia con la política de gestión de riesgos empresariales de la organización (de existir) y con la PSI. c) Asegurarse que la gestión de riesgos se encuentre perfectamente alineada con la cultura de la organización. d) Aprobar el proceso de gestión de riesgos de SI y, a su vez, asegurarse de que el mismo continúe siendo apropiado. e) Asegurar el compromiso de todos los niveles de la organización para la gestión de riesgos de SI.		
ISO 31.000 4.2 [6]		

GR1.2.15	Nivel C	F
Proceso de gestión de riesgos de SI		
El órgano rector de gobierno de la organización deberá definir el apetito de riesgo de la organización. El mismo deberá encontrarse definido en función de GR1.1.3 y GR 1.1.4. El apetito de riesgo de la organización debe: a) Reflejar los valores, objetivos estratégicos y recursos disponibles de la organización. b) Reflejar los requisitos legales, regulatorios, estatutarios y cualquier otro requisito al cual la organización suscribe y considere significativo. c) Ser mantenido y revisado periódicamente. d) Ser definido al inicio del proceso de gestión de riesgos de SI. e) Reflejarse dentro de la política de gestión de riesgos de SI y dentro del plan global de gestión de riesgos de SI. f) Reflejarse dentro de la estrategia de SI de la organización. g) Definir cómo deben analizase combinaciones de múltiples riesgos. h) Determinar el nivel al cual un riesgo se convierte en aceptable o tolerable para la organización en función de: *I.* El cumplimiento o no de requisitos definidos en b). *II.* El impacto sobre un proceso de negocio considerado clave para la organización. *III.* La naturaleza y consecuencias del impacto que pudiese ocurrir. *IV.* Los puntos de vista de las partes interesadas. *V.* La probabilidad de ocurrencia del impacto. *Se recomienda que el órgano rector de gobierno establezca una serie de recomendaciones o guías sobre cómo medir el impacto y la probabilidad de los riesgos de SI para de esta forma unificar la visión de niveles tolerables o aceptables de riesgo entre el gobierno y la gestión.*		
GR1.1.3 – GR1.1.4		

GR1.2.16	Nivel C	F
Proceso de gestión de riesgos de SI		
Con el objetivo de asegurar que la gestión del riesgo continua tanto siendo efectiva como apoyando la concreción de los objetivos estratégicos de la organización, la misma deberá: a) Revisar regularmente (a un intervalo no inferior a 12 meses) la eficiencia y efectividad de la gestión de riesgos de SI, el proceso de gestión de riesgos de SI y el Marco de Referencia de gestión de riesgos de SI en función de GR1.2.11. b) Revisar regularmente (a un intervalo no inferior a 12 meses) la eficiencia y efectividad de la gestión de riesgos de SI, el proceso de gestión de riesgos de SI y el Marco de Referencia de gestión de riesgos de SI para asegurarse que continúan siendo apropiados en función del contexto tanto interno como externo de la organización. c) Revisar tanto el progreso de como si continua siendo apropiado el plan global de gestión de riesgos de SI de la organización. d) Revisar el grado de cumplimiento de la política de gestión de riesgos de SI. e) Revisar la efectividad y periodicidad del reporte de riesgos a la alta dirección y al órgano rector de gobierno de la organización. *La implementación del presente apartado será responsabilidad del RMO. No obstante, el CSI permanecerá siendo un responsable estratégico del cumplimiento de dicho requerimiento.*		
ISO 31.000 4.5 [6]		

GR1.2.17	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá implementar mecanismos de comunicación interna y reporte con el objetivo de apoyar y alentar la responsabilidad y autoridad relativa a riesgos (EGR, RMO, RRs y demás autoridades de SI). Estos mecanismos deberán asegurar que: a) Los componentes del Marco de Referencia de gobierno de riesgos de SI, y cualquiera de sus modificaciones, sean comunicadas apropiadamente.		

b) Haya un adecuado reporte interno sobre la performance, efectividad y resultados del Marco de Referencia de gobierno de riesgos de SI de la organización.
c) Existan procesos de consulta e involucramiento de las partes interesadas internas.
d) La información relevante producto de la ejecución de la gestión de riesgos se encuentre disponible a niveles de la organización y tiempos apropiados.

Es recordable que estos mecanismos incluyan procesos que consoliden y centralicen la información vinculada a riesgos proveniente de diversas fuentes. Por otro lado, deberán analizar la sensibilidad de la información obtenida en función de LS2.3.6, con el objetivo de establecer controles y lineamientos de seguridad para la protección de esta.

ISO 31.000 4.3.6 [6]

GR1.2.18	Nivel C	F

Proceso de gestión de riesgos de SI

La organización deberá desarrollar, implementar y mantener un plan de comunicación con las partes interesadas externas. Dicho plan deberá establecer los lineamientos para:

a) El apropiado involucramiento de las partes interesadas externas con el objetivo de asegurar un intercambio efectivo de información con las mismas.
b) El reporte externo con el objetivo de cumplimentar ciertos requisitos legales, regulatorios, estatutarios, de mercado o de gobierno de la organización.
c) Proveer retroalimentación y reporte en consultas y comunicaciones.
d) Utilizar la comunicación con el objetivo de construir confianza en la organización.
e) Comunicarse con las partes interesadas en eventos de crisis o contingencias.

Es recordable que estos mecanismos incluyan procesos que consoliden y centralicen la información vinculada a riesgos proveniente de diversas fuentes. Por otro lado, deberán analizar la sensibilidad de la información obtenida en función de LS2.3.6, con el objetivo de establecer controles y lineamientos de seguridad para la protección de esta.

ISO 31.000 4.3.7 [6]

GR1.2.19	Nivel B	F
Proceso de gestión de riesgos de SI		
El CEP: a) Pasará a ser el responsable del diseño, implementación y mejora del proceso de gestión de riesgos de SI. b) Deberá determinar KPIs de la gestión de riesgos de SI que se encuentren perfectamente alineados a los KPIs organizacionales. El CEP medirá la performance del EGR en función de dichos KPIs y elevará el reporte al CSI.		
ISO 31.000 4.2 [6]		

GR1.2.20	Nivel B	F
Proceso de gestión de riesgos de SI		
La organización deberá diseñar un marco de referencia de gobierno de riesgos de SI en función de lo establecido en GR1.2.1, GR1.2.2, GR1.2.9 y en el presente requerimiento. En base a GR1.2.2 y GR1.2.9, el Marco de Referencia de Gestión de Riesgos de SI deberá contener los siguientes componentes fundamentales: a) Compromiso y mandato. b) Diseño del Marco de Referencia de Gestión de Riesgos de SI. VIII. *Entendimiento de la organización y su contexto.* IX. *Establecimiento de una política de gestión de riesgos.* X. *Responsabilidad y autoridad.* XI. *Integración con los procesos de la organización.* XII. *Recursos.* XIII. *Comunicación interna y reporte.* XIV. *Comunicación externa y reporte.*		

c) Implementación de la gestión de riesgos de SI.

III. Implementación del marco de referencia de gestión de riesgos de SI.

IV. Implementación del proceso de gestión de riesgos de SI.

d) Monitoreo y revisión del Marco de referencia de Gestión de Riesgos de SI.

e) Mejora continua del *Marco de referencia* de Gestión de Riesgos de SI.

La organización creará su propio marco de referencia en función de sus necesidades, la naturaleza de su negocio, su estructura organizacional y su cultura. No obstante, deberá adaptar, en la forma más conveniente a su naturaleza, los componentes del presente requerimiento.

Se recomienda que la organización tome como base su actual marco de referencia de gestión de riesgos de SI (de existir).

Se incluye a continuación la figura 1 de la norma ISO 31.000 incluida en la sección 0 de dicha norma a fines de facilitar la comprensión del presente requerimiento:

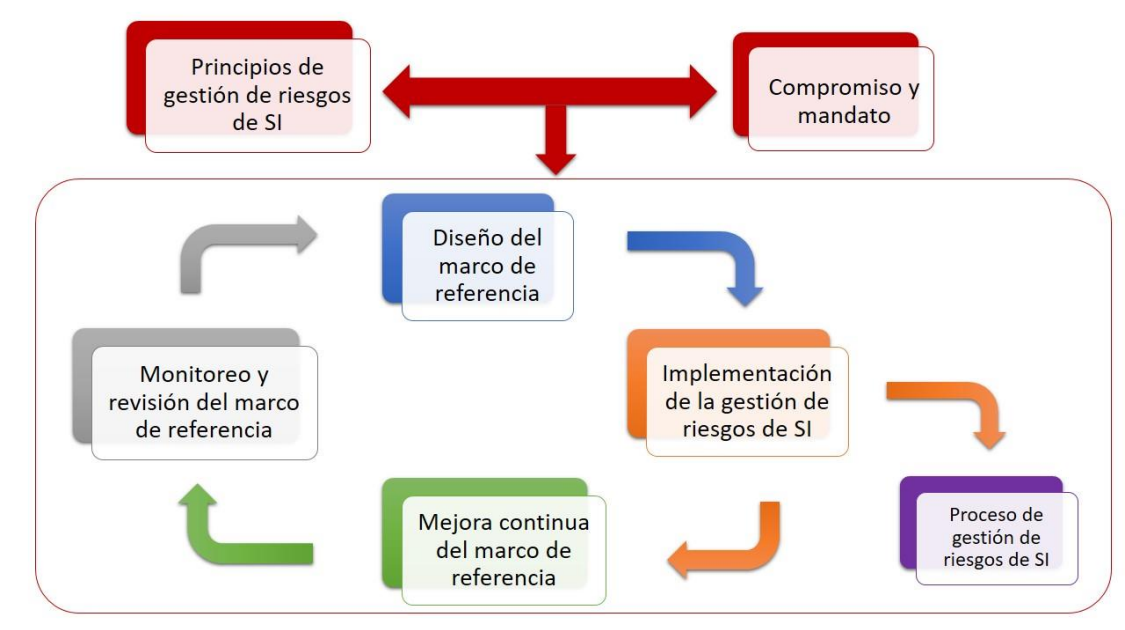

Ilustración GR1.2.20.A: Figura 1 de la norma ISO 31.000, sección 0.

ISO 31.000 4.1 y 4.6 [6]

GR1.2.21	Nivel B	F

Proceso de gestión de riesgos de SI

La organización deberá establecer una estructura de gobierno de riesgos de SI que se adecue a lo establecido en GR1.1.1, GR1.1.9, GR1.1.14, GR1.2.9, GR1.2.19 y GR1.2.20. Dicha estructura deberá a su vez diseñarse en forma de cascada según puede visualizarse en la ilustración GR1.2.21.A.

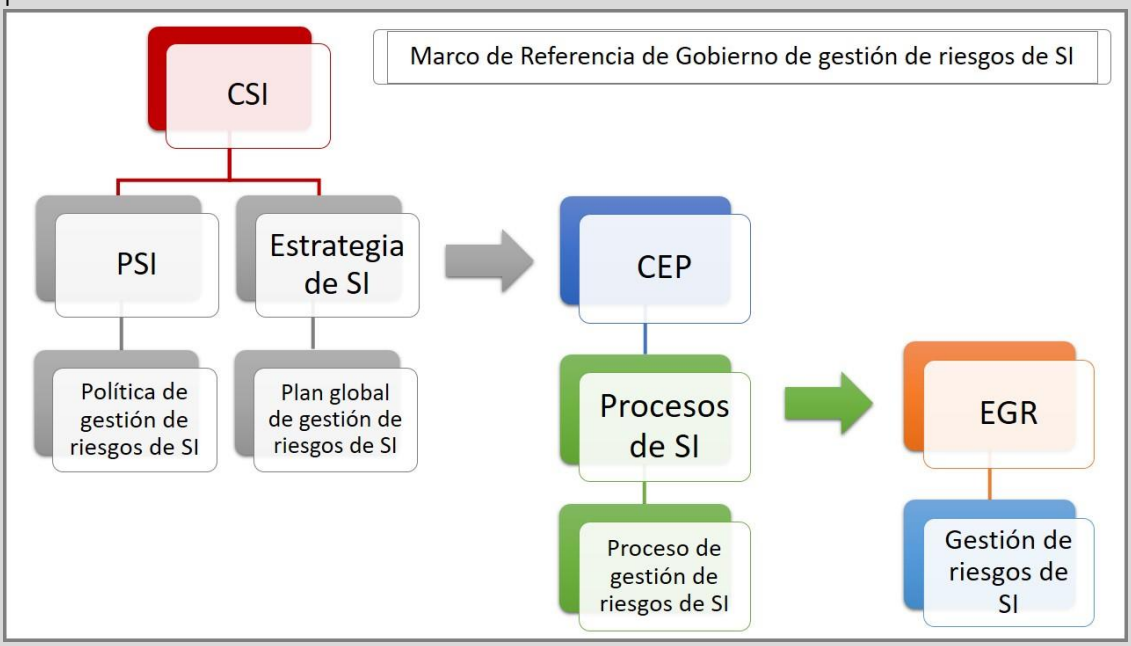

Ilustración GR1.2.10.A: Estructura modelo de gobierno de riesgos de SI.

ISO 31.000 4.3.3 [6]

GR2 PROCESO DE GESTIÓN DE RIESGOS DE SI

GR2.1 Lineamientos del proceso de Gestión de Riesgos

Objetivo Establecer los principios rectores del proceso de gestión de riesgos de seguridad de la información. Logrando, de esta forma sentar las bases del mismo: sus correspondientes subprocesos, sus responsables y el contexto en el cual debe ser diseñado, ejecutado y mantenido.

GR2.1.1	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá definir, aplicar, mantener y mejorar un proceso de gestión de riesgos de SI. La organización deberá asegurarse que el proceso de gestión de riesgos de SI sea aplicado a través del plan global de gestión de riesgos de SI (establecido en GR1.2.7) y a su vez, se encuentre alineado con todos los requerimientos establecidos en GR2.		
ISO 31.000 4.4.2 [6] – ISO 27.001 6.1.2 [1]		

GR2.1.2	Nivel D	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos de SI deberá: a) Ser estructurado y consistente en el tiempo. El mismo puede sufrir modificaciones con el objetivo de mejorarlo, no obstante, deberá existir una única versión estructurada del mismo para toda la organización. b) Ser una parte integrada a la gestión de la organización. No deberá ser un proceso más de la organización, sino que deberá encontrarse integrado con las demás actividades de esta. c) Encontrarse embebido en las prácticas y cultura de la organización. d) Encontrarse adaptado a la naturaleza del negocio de la organización.		
ISO 31.000 4.4.2 [6]		

GR2.1.3	Nivel D	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos de SI comprenderá los siguientes subprocesos: a) Establecimiento del contexto (GR1.1.6 y GR2.1.4). b) Evaluación del riesgo (GR2.2). c) Tratamiento del riesgo (GR2.3). d) Monitoreo y revisión (GR2.4).		
ISO 31.000 4.4.2 [6]		

GR2.1.4	Nivel D	F
Proceso de gestión de riesgos de SI		
El subproceso de establecimiento del contexto deberá basarse en lo detallado en GR1.1.6 y el presente requerimiento. El contexto deberá incluir: a) Recursos requeridos. b) Responsabilidades y autoridades. c) Documentación de soporte a la gestión de riesgos que debe ser almacenada. d) Los objetivos, las estrategias y la naturaleza del negocio de la organización. e) Las metodologías de evaluación e identificación de riesgos. f) La definición de los objetivos de la gestión de riesgos de SI de la organización. g) La definición del alcance de las actividades de gestión de riesgos (que debe encontrarse en concordancia con lo definido en GR1.1.6). Toda inclusión o exclusión específica debe quedar documentado en la política de gestión de riesgos. h) Identificando y especificando las decisiones que deben tomarse en materia de riegos de SI.		
ISO 31.000 5.3.4 [6]		

GR2.1.5	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá asegurar que las evaluaciones periódicas de riesgos de SI produzcan resultados coherentes, válidos y comparables. De esta forma, todas las actividades del proceso de gestión de riesgos de SI deberán ser trazables. Por lo tanto, dicho proceso generará registros que serán utilizados para su mejora continua en el tiempo. La organización deberá tomar en cuenta lo siguiente a la hora de la implementación y creación de dichos registros:		

a) Las necesidades de registros de los diferentes requisitos regulatorios, legales, operativos, estatutarios, entre otros identificados dentro del contexto de la gestión de riegos de SI de la organización. b) Los métodos de acceso y almacenamiento de los registros. c) La facilidad de recuperación de los registros. d) La sensibilidad de la información que contendrán dichos registros (en función de LS2.3.6).
ISO 31.000 5.7 [6] – ISO 27.001 6.1.2.b [1]

GR2.1.6	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá asegurarse que el proceso de gestión de riesgos sea desarrollado, ejecutado y mantenido en forma que cumplimente con las directivas del marco de referencia de gobierno de riesgos de SI diseñado por la misma (referirse a GR1.2.9).		
ISO 31.000 4.4.2 [6]		

GR2.1.7	Nivel C	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos de SI deberá: a) Encontrarse totalmente integrado a los procesos de negocio de la organización. b) Encontrarse estrechamente integrado a la toma de decisiones de SI.		
ISO 31.000 4.4.2 [6]		

GR2.1.8	Nivel C	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos de SI comprenderá los siguientes subprocesos: a) Establecimiento del contexto (GR1.1.6, GR2.1.4 y GR2.1.8). b) Evaluación del riesgo (GR2.2). c) Tratamiento del riesgo (GR2.3). d) Monitoreo y revisión (GR2.4). e) Comunicación e involucramiento (GR2.4).		
GR1.1.6 – GR2.1.4 – GR2.1,8 – GR2.2 – GR2.3 – GR2.4		
ISO 31.000 4.4.2 [6]		

GR2.1.9	Nivel C	F
Proceso de gestión de riesgos de SI		
El subproceso de establecimiento del contexto deberá basarse en lo detallado en GR1.1.6, GR2.1.4 y el presente requerimiento. El contexto deberá incluir: a) El alcance y los parámetros de los procesos de negocio de la organización. b) El Marco de Referencia de Gobierno de la organización. c) La cultura, prácticas y políticas de la organización. d) La definición de las relaciones entre proyectos o procesos particulares y otros proyectos o procesos de la organización. e) La identificación, descripción y definición del alcance, objetivos y recursos necesarios para realizar estudios de riesgos.		
ISO 31.000 5.3.4 [6]		

GR2.1.10	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá tomar en cuenta lo siguiente a la hora de la implementación y creación de los registros establecidos en GR2.1.5: a) El periodo de retención de estos. b) Esfuerzos y costos involucrados en la creación y mantenimiento de registros. c) Los beneficios de la reusabilidad de la información para propósitos de gestión.		
ISO 31.000 5.7 [6]		

GR2.1.11	Nivel B	F
Proceso de gestión de riesgos de SI		
El proceso de gestión de riesgos de SI comprenderá los siguientes subprocesos: a) Establecimiento del contexto (GR1.1.6, GR2.1.4, GR2.1.8 y GR1.1.12). b) Evaluación del riesgo (GR2.2). c) Tratamiento del riesgo (GR2.3). d) Monitoreo y revisión (GR2.4). e) Comunicación e involucramiento (GR2.4).		
ISO 31.000 4.4.2 [6]		

GR2.1.12	Nivel B	F
Proceso de gestión de riesgos de SI		
La organización deberá tomar en cuenta lo siguiente a la hora de la implementación y creación de los registros establecidos en GR2.1.5 y GR2.1.10: a) Las necesidades de la organización vinculadas a la mejora y al aprendizaje continuo.		
ISO 31.000 5.7 [6]		

GR2 PROCESO DE GESTIÓN DE RIESGOS DE SI

GR2.2 Evaluación de Riesgos

Objetivo Establecer el subproceso de evaluación de riesgos de seguridad de la información y asegurarse que el mismo se encuentre alineado a los lineamientos del Marco de Referencia de gobierno de gestión de riesgos de SI y al apetito de riesgos de la organización.

GR2.2.1	Nivel D	F
Subproceso de evaluación de riesgos de SI		
La organización deberá diseñar, ejecutar y mantener un subproceso de evaluación de riesgos. El cual deberá respetar todos los lineamientos establecidos en GR2.2. Dicho subproceso constara de tres componentes: a) Identificación de riesgos. b) Análisis de riesgos. c) Evaluación de riesgos. La siguiente ilustración detalla cómo se encuentran vinculados cada uno de estos componentes.		

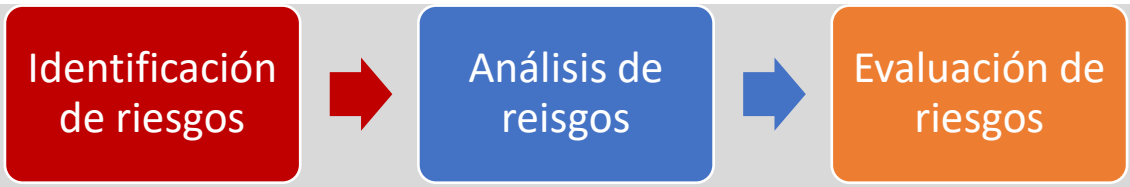

Ilustración GR2.2.1.A: Componentes del subproceso de evaluación de riesgos.

ISO 31.000 5.4.2 [6]

GR2.2.2	Nivel D	F

Subproceso de identificación de riesgos de SI

El EGR deberá identificar fuentes de riesgo y posibles áreas de impacto en función de las causas y consecuencias (impacto) de potenciales eventos que afecten la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

La identificación deberá abarcar todos los riesgos sin importar si su origen se encuentra o no bajo el control de la organización. A su vez, la identificación de riesgos deberá identificar a los RRs (responsables de riesgos, mencionados como "*propietarios de los riesgos*" en el apartado 6.1.2.c.2 de la norma ISO 27.001 [1]) de cada riesgo.

El objetivo del presente requerimiento consiste en la generación de un listado exhaustivo de riesgos de SI tomando como base aquellos eventos que podrían acelerar, retrasar, prevenir u obstaculizar el cumplimiento de los objeticos estratégicos de la organización.

ISO 31.000 5.4.2 [6] – ISO 27.001 6.1.2.c

GR2.2.3	Nivel D	F
Subproceso de identificación de riesgos de SI		
El EGR deberá identificar posibles causas y escenarios de riesgos que muestren a su vez las consecuencias (impacto del riesgo) que estos tienen sobre la organización o sobre su entorno. Todas las causas y consecuencias significativas deberán ser identificadas y documentadas. A su vez, deberá considerar la posibilidad de existencia de múltiples causas y/o consecuencias. A su vez, se debe ahondar en la posibilidad del efecto que ciertas consecuencias puedan tener al provocar efectos acumulativos o en cascada. Las consecuencias pueden ser expresadas en términos de impactos tangibles o intangibles. *Las consecuencias y sus probabilidades de ocurrencia pueden ser determinadas a través de la construcción de modelos del impacto o un conjunto de impactos de un cierto riesgo. A su vez, puede utilizarse información disponible o realizar una extrapolación de estudios técnicos o experimentales.*		
ISO 31.000 5.4.2 [6]		

GR2.2.4	Nivel D	F
Subproceso de análisis de riesgos de SI		
El EGR deberá analizar los riesgos de SI identificados en GR2.2.2. El análisis de riesgos deberá ser consistente y encontrarse alineado con: a) El apetito de riesgos determinado por la organización. b) El Marco de Referencia de gestión de riesgos de SI de la organización. c) El plan global de gestión de riesgos de SI de la organización. d) La política de gestión de riesgos de SI de la organización. La forma en que las consecuencias (el impacto del riesgo) y la probabilidad de ocurrencia de estas son expresadas y documentadas por la organización deberá ser consistente con el apetito de riesgos determinado por la organización.		

El mecanismo utilizado por la organización para combinar el impacto y la probabilidad de los riesgos a fin de determinar su nivel deberá ser consistente con el apetito de riesgos determinado por la organización.

El objetivo del presente requerimiento consiste en asegurar que dentro del análisis de riesgos realizado por la organización se tomen en cuenta y se implementen todos los lineamientos que gobiernan la gestión de riesgos de SI.

ISO 31.000 5.4.3 [6] – ISO 27.001 6.1.2.d [1]

GR2.2.5	Nivel D	F

Subproceso de identificación de riesgos de SI

Deberá documentarse y comunicarse las situaciones en las que durante el análisis de riesgos:

a) Se genere divergencia de opción entre expertos.
b) Se posea limitaciones en el modelado de la situación o el impacto riesgo.
c) Se cuente con incertidumbre, baja calidad, poca cantidad y/o nula relevancia de información necesaria para tomar una decisión respecto a un cierto riesgo.
d) Se cuente con la disponibilidad, cantidad, calidad y/o relevancia de información necesaria para tomar una decisión respecto a un cierto riesgo.
e) La existencia de supuestos y/o precondiciones tomados a la hora de analizar un riesgo.

ISO 31.000 5.4.2 [6]

GR2.2.6	Nivel D	F

Subproceso de análisis de riesgos de SI

Al realizar el análisis de riesgos de SI de la organización, el EGR deberá:

a) Establecer las diferentes causas y fuentes del riesgo.
b) Establecer las consecuencias del riesgo (que podrían resultar en caso de su materialización) tanto sean positivas o negativas y la probabilidad de ocurrencia de dichas consecuencias.

c) Establecer los factores que afectan a las consecuencias (impacto) del riesgo.
d) Identificar y analizar todos los controles existentes para determinar si son apropiados, efectivos y suficientes.
e) Establecer el nivel del riesgo.

La organización deberá hacer especial hincapié en el análisis de la interdependencia entre diversos riesgos y sus correspondientes fuentes u orígenes.

ISO 31.000 5.4.3 [6] - ISO 27.001 6.1.2.d [1]

GR2.2.7	Nivel D	F

Subproceso de evaluación de riesgos de SI

El EGR deberá evaluar los riesgos que han sido identificados y posteriormente analizados en GR2.2.4.

El tercer componente del subproceso de evaluación de riesgos de SI (GR2.2.1) deberá enfocarse principalmente en comparar el nivel de riesgo, establecido durante la etapa de análisis de riesgos, con el apetito de riesgo de la organización (establecido en GR1.1.3) en función del contexto considerado y establecido en GR1.1.6.

Los riesgos deberán evaluarse en función de:

a) Su probabilidad de ocurrencia.
b) Sus posibles impactos.
c) El impacto a un proceso considerado como crítico por la organización.
d) La existencia de controles vinculados al riesgo.
e) La suficiencia y efectividad de los controles vinculados al riesgo.
f) El incumplimiento u obstaculización del cumplimiento de un requisito legal, regulatorio, estatutario u otro requisito identificado por la organización en GR1.1.6.

ISO 31.000 5.4.4 [6]

GR2.2.8	Nivel D	F
Subproceso de evaluación de riesgos de SI		
La evaluación de riesgos debe: a) Realizarse en concordancia con los requisitos legales, regulatorios, estatutarios, de mercado y todo otro requerimiento identificado por la organización dentro del contexto establecido en GR1.1.6). b) Incluir una consideración de la tolerancia vinculada al nivel de un cierto riesgo (tanto su causa sea interna o externa a la organización). c) Producir como resultado un documento que contenga el listado de todos los riesgos evaluados y ordenados según su prioridad. d) Determinar el nivel de cada uno de los riesgos evaluados y documentar dicha decisión. e) Priorizar los riesgos para su tratamiento. Todas las decisiones de riesgos deben documentarse y almacenarse por un plazo razonable para su revisión en los próximos ciclos de ejecución del proceso de gestión de riesgos de SI.		
ISO 31.000 5.4.4 [6] - ISO 27.001 6.1.2.d [1]		

GR2.2.9	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá a su vez identificar y evaluar los riesgos que se encuentren vinculados al costo de oportunidad. *De esta forma no se centrará únicamente en aquellos riesgos cuyo impacto sea completamente negativo.*		
ISO 31.000 5.4.2 [6]		

GR2 PROCESO DE GESTIÓN DE RIESGOS DE SI

GR2.3 Tratamiento de Riesgos

Objetivo Establecer el subproceso de tratamiento de riesgos de seguridad de la información y asegurarse que el mismo se encuentre alineado a los lineamientos del Marco de Referencia de gobierno de gestión de riesgos de SI y al apetito de riesgos de la organización.

GR2.3.1	Nivel D	F
Subproceso de tratamiento de riesgos de SI		
La organización deberá diseñar, ejecutar y mantener un subproceso de tratamiento de riesgos. El cual deberá respetar todos los lineamientos establecidos en GR2.3. Dicho subproceso constara de tres componentes: a) Evaluación de tratamiento de riesgo. b) Decisión de aceptación o no aceptación del riesgo. c) Selección de opciones de tratamiento de riesgos. d) Evaluación del riesgo residual. e) Preparación e implementación de planes de tratamiento de riesgos.		

La siguiente ilustración detalla cómo se encuentran vinculados cada uno de estos componentes.

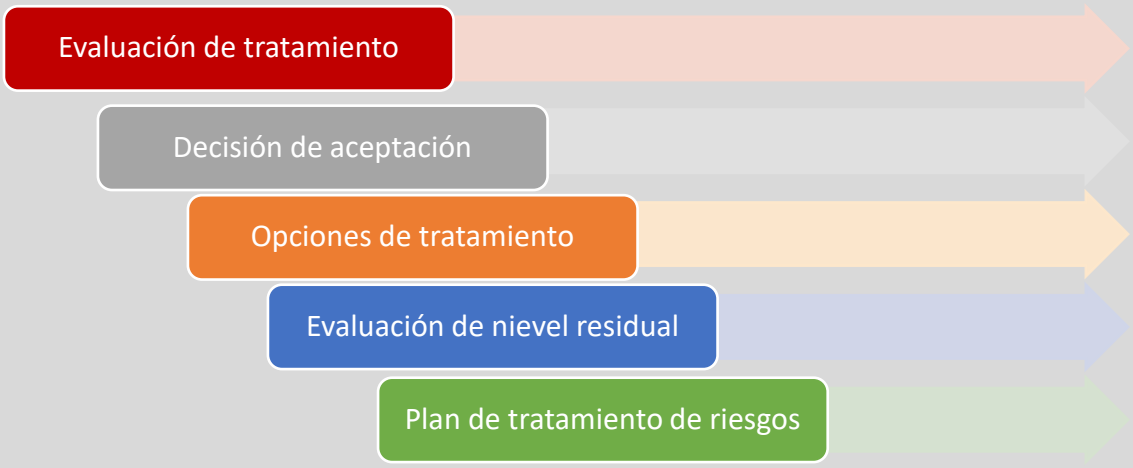

Ilustración GR2.3.1.A: Componentes del subproceso de tratamiento de riesgos.

ISO 31.000 5.5.1 [6]

GR2.3.2	Nivel D	F

Subproceso de tratamiento de riesgos de SI

La evaluación de tratamiento de riesgos GR2.3.1.a se realizará en función de lo generado por el último componente (evaluación de riesgos) de GR2.2.7 y GR2.2.8.

Se tomará como input el nivel de riesgo establecido en GR2.2.8. Dicho nivel deberá someterse a una evaluación por parte del EGR en función del apetito de riesgo de la organización. De dicha evaluación resultará una decisión de aceptación o no del riesgo inherente (GR2.3.1.b).

ISO 31.000 5.5.1 [6]

GR2.3.3	Nivel D	F

Proceso de gestión de riesgos de SI

El EGR deberá seleccionar una o varias opciones de tratamiento para aquellos riesgos que no hayan sido aceptados en GR2.3.2. Dichas opciones incluirán:

a) EVITAR el riesgo a través de la decisión de no comenzar o continuar con la actividad, proceso o proyecto que genera dicho riesgo.
b) APROVECHAR una oportunidad y tomar o incrementar el riesgo.
c) COMPARTIR el riesgo con un tercero o un conjunto de terceros.
d) REDUCIR la probabilidad de ocurrencia del riesgo.
e) REDUCIR las consecuencias (impacto) del riesgo.
f) PREVENIR el riesgo eliminando la fuente o causa del mismo.
g) PROTEGER[44] a los activos de información afectados por el riesgo [13].
h) RETENER el riesgo a través de una decisión informada.

Se debe recordar que las opciones de tratamiento de riesgo no son mutuamente excluyentes entre sí y que podrían no ser apropiadas en ciertas circunstancias.

La selección de las opciones de tratamiento de riesgos deberá incluir un balance que analice el costo/beneficio de la implementación de dicha opción, el cumplimiento de requerimientos legales, regulatorios, estatutarios u otros requerimientos identificados por la organización (tales como responsabilidad social y protección del medioambiente) y el impacto sobre procesos de negocio y sistemas de información considerados como críticos por la organización.

La organización debe prestar especial atención a aquellos riesgos cuyo tratamiento no sea justificable en términos económicos (el impacto del riesgo es más económico que la implementación del control) pero cuyo impacto no económico sea severamente negativo para la organización. En ciertas ocasiones la organización podría decidir implementar el control, aunque resultase en un costo mayor debido al gran impacto negativo que podría causar el riesgo (daño reputacional, ambiental, entre otros).

ISO 31.000 5.5.1 y 5.5.2 [6] – ISO 27.001 6.1.3.a [1]

[44] Algunas medidas de protección podrían ser: "*planes de emergencia o contingencia, equipos de protección personal para los RRHH, sistemas automáticos de protección*", entre otros [13].

GR2.3.4	Nivel D	F
Proceso de gestión de riesgos de SI		
Durante la aplicación del requerimiento GR2.3.3, el EGR deberá definir todos los controles que serán necesarios para la implementación de las opciones de tratamiento de riesgos de SI seleccionadas. *Dichos controles podrán responder a requerimientos del Sistema de Mejora Continua de SI o haber sido identificados de fuentes relevantes externas.* El EGR deberá comparar los controles que hayan sido determinados con todos los controles y lineamientos del MRU vinculados al estadio de madurez objetivo de la organización. De esta forma, deberá verificar y documentar que no se hayan omitido controles necesarios vinculados a su estadio de madurez del Sistema de Mejora Continua de SI. *La comparación de controles del presente requerimiento no se basa en la lista de controles y objetivos de control del Anexo A de la norma ISO 27.001 debido a que dicho listado no es exhaustivo y posee un alcance limitado en comparación con los controles y lineamientos del Modelo de Madurez de SI del MRU. Sin embargo, podrá tomarse como base de consulta de los controles mínimos e indispensables para el estadio de madurez "C".* El EGR deberá producir una Declaración de Aplicabilidad (en función del requerimiento 6.1.3.d de la norma ISO 27.001 [1]) que contenga los controles necesarios según lo definido por el presente requerimiento. Dentro de la Declaración de Aplicabilidad se deberán justificar las inclusiones (implementadas o no) y las exclusiones de los controles y lineamientos del MRU vinculados al estadio de madurez objetivo de la organización. La Declaración de Aplicabilidad deberá documentarse y almacenarse apropiadamente para su revisión, mejora y consulta periódica.		
ISO 27.001 6.1.3.b, 6.1.3.c y 6.1.3.d [1]		

GR2.3.5	Nivel D	F
Proceso de gestión de riesgos de SI		
El EGR deberá realizar una evaluación del riesgo residual (nivel de riesgo luego de la implementación de las opciones de tratamiento de riesgos de SI establecidas en GR2.3.3) en función del apetito de riesgo de la organización. De dicha evaluación resultará una decisión de aceptación o no del riesgo residual (GR2.3.1.d). *De no ser aceptado, se deberá definir la o las opciones de tratamiento de riesgo adicionales que deberán ser implementadas hasta que la organización considere el riesgo aceptable (en función de su apetito de riesgo).* El riesgo residual deberá ser documentado y encontrarse sujeto a revisiones periódicas para definir su evaluación y posible tratamiento en el futuro. El EGR deberá obtener la aceptación de los riesgos residuales por parte de los RRs de dicho riesgo. La aprobación deberá documentarse.		
ISO 31.000 5.5.1 [6] – ISO 27.001 6.1.3.f [1]		

GR2.3.6	Nivel D	F
Proceso de gestión de riesgos de SI		
Luego de haber aceptado el riesgo residual de los riesgos sujetos a análisis por el EGR, se deberá proceder a la confección de un plan de tratamiento de riesgos de SI. Dicho plan deberá detallar como se implementarán las opciones de tratamiento de riesgos seleccionadas al: a) Establecer las opciones de tratamiento de riesgos (diseño, implementación, mejora, eliminación o combinación de controles). b) Identificar claramente la prioridad en la que las opciones de tratamiento de riesgos individuales deben ser implementadas. c) Incluir las razones por la selección incluida en a) (incluyendo supuestos y beneficios que se esperan obtener con la implementación de dicha opción) d) Incluir tiempos y cronograma de implementación.		

e) Detallar al responsable por la aprobación del plan y el responsable de su mantenimiento e implementación. El plan de tratamiento de riesgos de SI deberá ser aprobado por los RRs. La aprobación deberá documentarse.
ISO 31.000 5.5.1 y 5.5.3 [6] – ISO 27.001 6.1.3.e [1]

GR2.3.7	Nivel D	F
Proceso de gestión de riesgos de SI		
De surgir riesgos secundarios asociados al tratamiento de un cierto riesgo, dichos riesgos secundarios deberán: a) Ser analizados, evaluados y tratados. b) Ser monitoreados y revisados periódicamente. c) Ser incorporados al mismo plan de tratamiento de riesgos vinculados al riesgo primario. No deberán ser tratados como nuevos riesgos aislados del riesgo primario. El vínculo entre los riesgos primarios y secundarios deberá ser identificado, documentado y mantenido en el tiempo.		
ISO 31.000 5.5.1 [6]		

GR2.3.8	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá implementar el plan de tratamiento de riesgos de Seguridad e la Información detallado en GR2.3.6. A su vez, deberá conservar información documentada sobre el diseño y los resultados de la implementación, mantenimiento y mejora de dicho plan.		
ISO 27.001 8.3 [1]		

GR2.3.9	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización deberá considerar los valores y las percepciones de las partes interesadas, como asa también los mecanismos apropiados de comunicación con las mismas, a la hora de seleccionar opciones de tratamiento de riesgos. Cuando las opciones de tratamiento de riesgos impactasen algún área funcional o proceso de la organización, los RGs o RPs vinculados deberán ser involucrados en la toma de decisiones. Cuando las opciones de tratamiento de riesgos impactasen sobre alguna parte interesada, estos deberán ser involucrados en la toma de decisiones. Cuando las opciones de tratamiento de riesgos impactasen sobre algún activo de información de la organización, los RAIs vinculados a los mismos deberán ser involucrados en la toma de decisiones.		

GR2.3.10	Nivel C	F
Proceso de gestión de riesgos de SI		
El plan de tratamiento de riesgos de SI de la organización deberá: a) Incluir los requerimientos de reporte y monitoreo de la gestión de riesgos de SI. b) Incluir las medidas y restricciones de performance. c) Incluir los recursos requeridos y necesarios (incluyendo contingencias). d) Encontrarse integrado con los procesos de gestión de la organización. e) Ser discutido y evaluado con las partes interesadas apropiadas.		
ISO 31.000 5.5.3 [6]		

GR2.3.11	Nivel B	F
Proceso de gestión de riesgos de SI		
El plan de tratamiento de riesgos de SI deberá ser aprobado por el CEP.		

GR2 PROCESO DE GESTIÓN DE RIESGOS DE SI

GR2.4 Monitoreo y mejora continua

Objetivo Establecimiento del subproceso de monitoreo y mejora continua de la gestión de riesgos de SI de la organización, para así dotar a la misma de la capacidad de conocer y adecuar continuamente su habilidad para gestionar de forma óptima sus riesgos de SI.

GR2.4.1	Nivel D	F
Proceso de gestión de riesgos de SI		
La organización deberá diseñar, ejecutar y mantener un subproceso de monitoreo y mejora continua de la gestión de riesgos de SI. El cual deberá respetar todos los lineamientos establecidos en GR2.4. El monitoreo y la revisión de la gestión de riesgos de SI de la organización debe realizarse en forma estructurada y planeada a través del presente subproceso. Dicho monitoreo y revisión permitirán a la organización realizar una mejora continua de la gestión de riesgos.		
ISO 31.000 5.6 [6]		

GR2.4.2	Nivel D	F
Proceso de gestión de riesgos de SI		
El subproceso establecido en GR2.4.1 deberá: a) Ser ejecutado periódicamente. b) Ser ejecutado por actores que posean la responsabilidad y autoridad necesaria para llevar adelante las actividades requeridas por el mismo. c) Alcanzar a todo el proceso de gestión de riesgos de SI de la organización. d) Asegurar que los controles establecidos e implementados a través del proceso de gestión de riesgo de SI sean suficientes, apropiados, eficientes y efectivos tanto en su diseño como en su operación. e) Detectar cambios tanto en el contexto interno como en el externo. f) Detectar cambios en riesgos individuales que requieran la revisión del plan de tratamiento de riesgos de SI y sus respectivas prioridades establecidas. Las responsabilidades y la autoridad detalladas en b) deberán formar encontrarse claramente detalladas dentro de la política de gestión de riesgos de SI de la organización y su vez, encontrarse alineadas al Marco de Referencia de gestión de riesgos de SI de la organización.		
ISO 31.000 5.6 [6]		

GR2.4.3	Nivel C	F
Proceso de gestión de riesgos de SI		
El subproceso establecido en GR2.4.1 y GR2.4.2 deberá a su vez: a) Encontrarse diseñado para recabar información que colabore con la mejora de la gestión de riesgos de SI de la organización. b) Identificar riesgos emergentes. c) Priorizar el análisis de eventos, cambios, tendencias, sucesos, errores y fallas vinculadas a la organización y su contexto con el objetivo aprender sobre los mismos y evitar que sus consecuencias afecten negativamente a la organización.		
ISO 31.000 5.6 [6]		

GR2.4.4	Nivel C	F
Proceso de gestión de riesgos de SI		
Se deberá abordar el involucramiento de y la comunicación con todas las partes interesadas tanto externas como internas durante todas las etapas del proceso de gestión de riesgos de SI.		
ISO 31.000 5.2 [6]		

GR2.4.5	Nivel C	F
Proceso de gestión de riesgos de SI		
La organización desarrollará planes de comunicación e involucramiento de las partes interesadas a fin de cumplir con GR2.4.2. Dichos planes deberán abordar: a) Las cuestiones vinculadas al riesgo vinculado a la parte interesada. b) Las causas de dicho riesgo. c) Las consecuencias posibles (si son conocidas). d) Las medidas que la organización ha tomado para tratar dicho riesgo. e) El involucramiento de las partes interesadas para: I. Colaborar en la correcta identificación de riesgos. II. Asegurarse que los intereses de las partes interesadas son considerados y comprendidos. III. Colaborar en el correcto establecimiento del contexto. IV. Reunir a diferentes áreas de conocimiento a la hora de gestionar riesgos con el objetivo de asegurar que se consideran diversos puntos de vista durante la evaluación de riesgos (ya que las percepciones de riesgo variaran entre las distintas partes interesadas). V. Asegurar el apoyo y aprobación del plan de tratamiento de riesgos de SI. *Se recomienda que los planes sean desarrollados en forma temprana por la organización para facilitar el desarrollo del proceso de gestión de riesgos.* *El objetivo del presente requerimiento consiste en establecer una comunicación efectiva entre quienes gestionan los riesgos y las partes interesadas de la*		

organización, para que estas últimas comprendan el contexto en el cual se toman las decisiones y las razones particulares por las que ciertas acciones son requeridas.
ISO 31.000 5.2 [6]

GR2.4.6	Nivel B	F
Proceso de gestión de riesgos de SI		
Para el logro de una efectiva mejora continua, la organización deberá establecer metas y objetivos de performance para la gestión de sus riesgos de SI. A su vez, deberá periódicamente medir, revisar y si lo cree conveniente modificar los procesos, sistemas, recursos, capacidades y habilidades vinculadas a la gestión de riesgos de SI de la organización. *La revisión periódica de la performance gestión de riesgos establecida en el presente requerimiento no deberá exceder los 12 meses entre cada una de sus ejecuciones.*		
ISO 31.000 Anexo A A.3.1 [6]		

GR2.4.7	Nivel B	F
Proceso de gestión de riesgos de SI		
La performance de la organización en materia de gestión de riesgos de SI deberá ser publicada y comunicada a todas las partes interesadas apropiadas. Dicha comunicación deberá realizarse en función de lo establecido en GR2.2.4 y GR2.2.5.		
ISO 31.000 Anexo A A.3.1 [6]		

GR2.4.8	Nivel B	F
Proceso de gestión de riesgos de SI		
La gestión de riesgos de SI de la organización deberá abarcar comunicaciones continuas con las partes interesadas internas y externas. Dichas comunicaciones incluirán el reporte frecuente y comprensivo de la performance de la gestión de riesgos de SI. LA comunicación con las partes interesadas deberá ser implementada como un proceso de dos vías. Por lo que la organización deberá fomentar el involucramiento de las partes interesadas a través del análisis de sus recomendaciones y retroalimentación de la performance de la gestión de riesgos de SI.		
ISO 31.000 Anexo A A.3.4 [6]		

[Página dejada en blanco intencionalmente]

INGENIERÍA DE SEGURIDAD

El objetivo primordial del presente subsistema comprende el establecimiento de los lineamientos principales de la Seguridad de la Información.

Se enfoca principalmente en el diseño de una metodología base de seguridad que englobe los aspectos primordiales de la seguridad física y ambiental, el otorgamiento, mantenimiento y supresión de accesos a los activos de información de la organización y en la defensa de estos a través de la gestión de los incidentes de Seguridad de la Información.

IS1 Controles Generales de Seguridad de la Información

IS1.1 Seguridad Física y Ambiental

IS1.2 Uso de Activos de Información

IS1.3 Gestión de accesos

IS2 Protección y Defensa de los Activos de Información

IS2.1 Protección de la información

IS2.2 Gestión de incidentes de Seguridad de la Información

IS1 CONTROLES GENERALES DE SEGURIDAD

IS1.1 Seguridad Física y Ambiental

Objetivo Establecer los fundamentos de la seguridad física y ambiental en función de los lineamientos delineados por la documentación fuente del MRU. El Presente Dominio de Seguridad será regularmente utilizado como "*quick win*" por los especialistas de seguridad para que el negocio logre visualizar su trabajo.

IS1.1.1	Nivel E	F
Proceso de implementación de áreas restringidas		
La organización debe definir y utilizar perímetros de seguridad para proteger áreas que contengan información e instalaciones de procesamiento de información sensibles o críticas (áreas que gestionen, almacenen o trabajen con información clasificada con sensibilidad ALTA o CRÍTICA por la organización). Dichas áreas serán clasificadas como áreas restringidas. Las áreas restringidas deberán: a) Ser físicamente seguras. b) Poseer un área de recepción atendida por personas u otros medios de control de acceso físico al sitio o al edificio. El objetivo de esta área consiste en restringir el acceso exclusivamente al personal autorizado a los distintos sitios y edificios.		

c) Encontrarse protegidas por barreras físicas para prevenir el acceso físico y la contaminación del entorno.
d) Poseer puertas de incendio con alarmas, que operen de acuerdo con las reglamentaciones legales pertinentes en cuanto a seguridad contra incendios de manera tal de asegurar la seguridad de las personas en caso de falla.
e) Poseer sistemas de detección de intrusos según normas nacionales, regionales o internacionales que cubran todas las puertas exteriores y las ventanas accesibles. Las áreas desocupadas (por ejemplo, el centro de cómputos) deberán poseer alarmar activadas en forma permanente.

No deberán existir brechas en el perímetro de las áreas restringidas donde pueda ocurrir fácilmente una irrupción. Las paredes, el techo y el piso exteriores del área restringidas deberán ser de construcción sólida y, todas las puertas exteriores deberán estar adecuadamente protegidas contra accesos no autorizados con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). A su vez, las puertas y ventanas deberán encontrarse trabadas cuando queden sin supervisión.

Todo edificio o instalación que posee un área restringida deberá poseer una protección externa en todas sus ventanas (como mino hasta aquellas pertenecientes al tercer piso de la estructura) y puertas que den al exterior.

En función de d), las puertas de incendio deberán ser monitoreadas y probadas en conjunto con las paredes para establecer el nivel requerido de resistencia de acuerdo con las normas nacionales, regionales e internacionales adecuadas.

Se deberán probar regularmente los sistemas de detección detallados en e).

LS2.3.6
ISO 27.001 A.11.1.1 [1] - ISO 27.002 11.1.1 [14]

IS1.1.2	Nivel E	F
Proceso de implementación de áreas restringidas		
La organización debe proteger las áreas restringidas mediante controles de ingreso apropiados para asegurar que solo se permita el acceso al personal autorizado.		

La aplicación del presente requerimiento deberá tener en cuenta los siguientes lineamientos:

a) Se deberá registrar la fecha y hora tanto de entrada como de salida de las visitas.
b) Se deberán supervisar a todas las visitas, desde su ingreso hasta su salida al área restringida.
c) Las visitas podrán únicamente ingresar en función de propósitos específicos y autorizados.
d) Se deberá restringir el acceso a las, sólo a personas autorizadas mediante la implementación de al menos dos controles de acceso (por ejemplo: mecanismos de autenticación de dos factores tales como tarjetas de acceso y un número de identificación personal, PIN, secreto). Dichas áreas deberán a su vez poseer una vigilancia permanente combinando equipamiento tecnológico (alarmas, cámaras de seguridad, sensores, entre otros) y recursos humanos (personal de seguridad y similares).
e) Se deberá llevar un libro físico y digital de registros de accesos al área restringidas para el caso de las visitas. Para el personal de ingreso habitual a las áreas restringidas podrá utilizarse solo uno de estos mecanismos (físico o digital).
f) Se deberán revisar y actualizar periódicamente los derechos de acceso a las áreas restringidas. Los accesos deberán revocarse cuando sea necesario (ante despido, suspensión, licencia o cambio de tareas o actividades de todo empleado, contratado o personal de terceras partes).

ISO 27.001 A.11.1.2 [1] – ISO 27.002 11.1.2 [14]

IS1.1.3	Nivel E	F

Proceso de implementación de áreas restringidas

La organización debe diseñar y aplicar seguridad física a las oficinas, recintos e instalaciones de toda la organización alcanzada por el Sistema de Mejora Continua en SI (en función del alcance establecido en LS1.1.4).

La aplicación del presente requerimiento deberá tener en cuenta los siguientes lineamientos:

a) Se deberán ubicar instalaciones clave de modo tal de evitar el acceso del público.

b) No se deberá permitir el acceso a personas no autorizadas a los directorios y listados internos de teléfonos que identifiquen la ubicación de las instalaciones de procesamiento de información confidencial.

ISO 27.001 A.11.1.3 [1] – ISO 27.002 11.1.3 [14]

IS1.1.4	Nivel E	F

Proceso de implementación de áreas restringidas

La organización debe controlar los puntos de acceso, tales como las áreas de carga y descarga y otros puntos donde personas no autorizadas podrían llegar a ingresar en las instalaciones y se deben aislar de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Para lo cual, la organización deberá:

a) Restringir el acceso a un área de carga y descarga desde el exterior del edificio únicamente a personal identificado y autorizado.
b) Diseñar el área de carga y descarga de manera tal que los suministros puedan ser cargados y descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Asegurar las puertas exteriores de un área de carga y descarga previa a la apertura de las puertas internas.
d) Inspeccionar y examinar el material entrante en busca de explosivos, químicos u otros materiales peligrosos antes de su traslado desde el área de carga y descarga.
e) Registrar el material entrante de acuerdo con los procedimientos de gestión de activos de información de la organización (referirse a LS2.3) previo a su ingreso a las instalaciones.
e) En la medida en que sea posible, separar físicamente de los envíos entrantes y salientes.
f) Inspeccionar el material entrante en busca de evidencia de alteración en tránsito. Si se descubriera dicha alteración, informar inmediatamente al personal de seguridad.

ISO 27.001 A.11.1.6 [1] – ISO 27.002 11.1.6 [14]

IS1.1.6	Nivel E	F
Subproceso de protección del equipamiento		
La organización deberá ubicar y proteger el equipamiento de manera tal que se reduzcan los riesgos ocasionados por amenazas y peligros del entorno y las oportunidades de acceso no autorizado. Para lo cual la organización deberá: a) Ubicar el equipamiento de modo tal que minimice el acceso innecesario a las áreas de trabajo. b) Posicionar cuidadosamente las instalaciones de procesamiento de información que manejan datos sensibles para reducir el riesgo de que personas no autorizadas vean la información durante su uso. c) Asegurar las instalaciones de almacenamiento para evitar el acceso no autorizado. d) Adoptar controles para minimizar el riesgo de potenciales amenazas físicas y del entorno (por ejemplo: robo, incendio, explosivos, humo, inundación, falta de suministro de agua, polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, interferencia en las comunicaciones, radiaciones electromagnéticas, vandalismo, entre otros). e) Establecer lineamientos en cuanto a comer, beber y fumar en las proximidades de las instalaciones de procesamiento de información. f) Monitorear las condiciones del entorno, como la temperatura y la humedad, para detectar condiciones que puedan afectar de manera adversa la operación en las instalaciones de procesamiento de información. g) Para el equipamiento en entornos industriales, considerar el uso de métodos especiales de protección, como teclados de membrana. j) Proteger el equipo que procesa información confidencial para minimizar el riesgo de fuga de información debido a las emanaciones electromagnéticas.		
ISO 27.001 A.11.2.1 [1] – ISO 27.002 11.2.1 [14]		

IS1.1.7	Nivel E	F
Subproceso de protección del equipamiento		
La organización deberá proteger al equipamiento de fallas en el suministro eléctrico o de otras interrupciones ocasionadas por fallas en elementos de		

soporte (tales como la electricidad, las telecomunicaciones, el suministro de agua, gas, cloacas, la ventilación y el aire acondicionado).

La organización deberá asegurar que todos los servicios de soporte:

a) Cumplan con las especificaciones del fabricante del equipamiento y con los requisitos legales locales.
b) Sean evaluados regularmente en función de su capacidad para cumplir con el crecimiento del negocio y sus interacciones con otros servicios de soporte.
c) Se inspeccionen y prueben regularmente para asegurar su funcionamiento apropiado.
d) Cuenten con una alarma para detectar su malfuncionamiento, de ser necesario.
e) Utilicen múltiples suministros con rutas físicas diferentes, de ser necesario. El suministro de telecomunicaciones deberá poseer al menos dos rutas físicas diferentes, a través de dos distintos proveedores.

La organización deberá proporcionar luces de emergencia dentro de todas sus instalaciones (que se encuentren dentro del alcance establecido en LS1.1.4) y, a su vez, servicios de telecomunicaciones de emergencia.

La organización deberá ubicar válvulas e interruptores de emergencia para la luz, al agua, el gas y otros servicios cerca de las salidas de emergencia o en las salas de equipamiento.

ISO 27.001 A.11.2.2 [1] – ISO 27.002 11.2.2 [14]

IS1.1.8	Nivel E	F

Subproceso de protección del cableado

La organización deberá proteger de intercepciones, interferencias y daños al cableado de suministro eléctrico y telecomunicaciones que transporten datos y/o que den soporte a servicios de información de la organización.

Para la implementación del presente requerimiento, la organización deberá:

a) Instalar las líneas de energía y telecomunicaciones que ingresan a las instalaciones de procesamiento de la información bajo tierra, cuando sea posible, o sujetas a una adecuada protección alternativa.

b) separar los cables de energía de los cables de comunicaciones para prevenir interferencias.

ISO 27.001 A.11.2.3 [1] – ISO 27.002 11.2.3 [14]

IS1.1.9	Nivel E	F

Subproceso de protección del equipamiento

La organización deberá asegurarse que su equipamiento reciba un mantenimiento correcto para asegurar su continua disponibilidad e integridad, en función de los siguientes lineamientos:

a) El mantenimiento del equipamiento debe realizarse de acuerdo con los intervalos y las especificaciones de servicio recomendados por el proveedor.
b) Sólo el personal de mantenimiento autorizado debe llevar a cabo reparaciones y mantenimiento del equipamiento.
c) Se debe registrar todas las fallas sospechadas o reales de todo el mantenimiento tanto preventivo como correctivo realizado.
d) Se deben implementar controles apropiados cuando esté programado el mantenimiento del equipamiento. Cuando sea posible, previo a la realización del mantenimiento, eliminar la información confidencial del equipamiento (a menos que el personal de mantenimiento posea la suficiente autorización y no se trate de personal de mantenimiento contratado o de un tercero).
e) Se deben cumplir con todos los requisitos de mantenimiento impuestos por las pólizas de seguro.
f) Previa a la puesta en funcionamiento del equipamiento luego del mantenimiento, se deberá inspeccionarlo para asegurar que no haya sido alterado y no funcione de manera incorrecta.

ISO 27.001 A.11.2.4 [1] – ISO 27.002 11.2.4 [14]

IS1.1.10	Nivel E	F
Subproceso de protección del cableado		
La organización deberá aplicar protección contra rayos en todos sus edificios y, a su vez, instalar filtros para la protección contra rayos en todas las líneas entrantes de energía y de telecomunicaciones.		
ISO 27.002 11.2.1 [14]		

IS1.1.11	Nivel D	F
implementación de áreas restringidas		
La organización deberá diseñar y aplicar la protección física contra desastres naturales, ataques intencionales o accidentes. *Se recomienda obtener asesoramiento especializado sobre las formas de evitar daños ocasionados por incendios, inundaciones, terremotos, explosiones, tumultos y otras formas de desastres naturales o antropogénicos.*		
ISO 27.001 A.11.1.4 [1] - ISO 27.002 11.1.4 [14]		

IS1.1.12	Nivel D	F
Proceso de implementación de áreas restringidas		
La organización deberá diseñar y aplicar procedimientos para el trabajo dentro de áreas restringidas. Dichos procedimientos deberán incluir controles para los usuarios (tanto empleados, contratistas y como de terceras partes) que abarquen todas las actividades desarrolladas dentro del área restringida. La aplicación del presente requerimiento deberá cumplir con los siguientes lineamientos:		

a) Que el personal sólo tenga conocimiento de la existencia de un área restringida, o de las actividades que se llevan a cabo dentro de ésta, en base a la necesidad de saber ("*need to know basis*"). b) Evitar el trabajo no supervisado en áreas restringidas tanto por razones de seguridad como para prevenir la posibilidad de que se lleven a cabo actividades maliciosas. c) La implementación de un bloqueo físico y la inspección periódica de las áreas seguras desocupadas. d) Que no se permitan equipos de fotografía, video, audio u otro tipo de equipamiento de grabación, tales como cámaras en dispositivos móviles, excepto que se los autorice.
ISO 27.001 A.11.1.5 [1] – ISO 27.002 11.1.5 [14]

IS1.1.13	Nivel D	F
Proceso de implementación de áreas restringidas		
La ubicación y la fortaleza de cada perímetro de seguridad detallado en IS1.1.1 dependerán de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una evaluación de riesgos. Se les deberá proveer las instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia, a las visitas que ingresen a áreas restringidas.		
ISO 27.002 11.1.1 y 11.1.2 [14]		

IS1.1.14	Nivel D	F
Proceso de implementación de áreas restringidas		
Las áreas restringidas deberán poseer múltiples barreras físicas de acceso que las cubran en su totalidad. A su vez, deberán poseer al menos un mecanismo de autenticación digital (biométrico, tarjetas de identificación, entre otros) y un mecanismo de seguridad humana (personal de seguridad).		

El uso de múltiples barreras brinda protección adicional, ya que la falla de una barrera no significa que la seguridad esté inmediatamente comprometida.
ISO 27.002 11.1.1 [14]

IS1.1.15	Nivel D	F
Proceso de implementación de áreas restringidas		
Se deberán implementar barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de acceso restringido (áreas restringidas). *Se debe prestar atención especial a la seguridad del acceso físico en el caso de edificios que contienen activos de múltiples organizaciones.*		
ISO 27.002 11.1.1 [14]		

IS1.1.16	Nivel D	F
Proceso de implementación de áreas restringidas		
Todos los empleados, contratistas y terceras partes que ingresen a un área restringida deberán utilizar alguna forma visible de identificación. La organización deberá exigir a todos los empleados, contratistas y terceras partes, la inmediata notificación al personal de seguridad en caso de encontrar alguna visita sin escolta o alguien que no utilice una identificación visible. Se deberá otorgar acceso a las áreas restringidas al personal de terceras partes que provean servicio de soporte solamente cuando se requiera con previa autorización y monitoreo continuo del acceso.		
ISO 27.002 11.1.2 [14]		

IS1.1.17	Nivel C	F
Subproceso de protección del equipamiento		
Se deberán separar las instalaciones de procesamiento de información gestionadas por la organización de aquellas gestionadas por terceras partes.		
ISO 27.002 11.1.1 [14]		

IS1.1.18	Nivel C	F
Proceso de implementación de áreas restringidas		
Las siguientes áreas deberán ser clasificadas como áreas restringidas para la organización: a) Centro de cómputos. b) Área de generador de energía. c) Área de almacenamiento de combustible. d) Área de monitoreo de cámaras, herramientas y personal de seguridad. e) Áreas de control y monitoreo de accesos. f) Áreas y sectores de infraestructura de energía, TICs y de cualquier otro servicio de soporte especificado en IS1.1.7. g) Sectores o áreas de almacenamiento físico o digital de información clasificada con sensibilidad CRÍTICA o ALTA. A su vez, la organización podrá clasificar como áreas restringidas a aquellas áreas que manejen, almacenen o gestionen información clasificada con sensibilidad MEDIA.		

IS1.1.19	Nivel C	F
Proceso de implementación de áreas restringidas		
Dentro de las áreas restringidas se deberán implementar los siguientes lineamientos:		

a) Los edificios deberán ser discretos y otorgar una mínima indicación posible de su propósito, sin señales obvias, tanto fuera como dentro del edificio, que identifiquen la presencia de actividades de procesamiento de información o actividades de alta sensibilidad de la organización.
b) Se deberán configurar las instalaciones de modo tal de prevenir que la información confidencial o las actividades se vean o escuchen desde el exterior de las áreas restringidas.
c) Considerar, cuando corresponda, el bloqueo electromagnético dentro de las áreas restringidas.
d) Establecer lineamientos en cuanto a comer, beber y fumar dentro y en las proximidades de las áreas restringidas.

ISO 27.002 11.1.3 y 11.2.1 [14]

IS1.1.20	Nivel C	F

Subproceso de protección del cableado

Complementando la protección contra intercepciones, interferencias y daños al cableado de suministro eléctrico y telecomunicaciones que transporten datos y/o que den soporte a servicios de información de la organización (detallado en IS1.1.8), la organización deberá implementar los siguientes lineamientos:

a) Instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
b) Uso de blindaje electromagnético para proteger el cableado; la realización de barridos técnicos e inspecciones físicas en busca de dispositivos que hayan sido acoplados a los cables sin autorización.
c) Acceso controlado a los paneles de conexión y a las salas de cableado.

ISO 27.002 11.2.3 [14]

IS1.1.21	Nivel B	F
Subproceso de protección del equipamiento		
Los lineamientos establecidos en IS1.1.7.d y IS1.1.7.e serán de carácter obligatorio para los siguientes servicios de soporte: a) Telecomunicaciones/TICS. En este caso se deberá contar con al menos dos proveedores distintos y cada uno de ellos deberá proveer por lo menos dos rutas físicas de suministro diferentes. b) Energía eléctrica. c) Aire acondicionado. d) Ventilación. e) Suministro de agua. Se sumará a la lista el suministro de gas únicamente si la organización lo utiliza para el desarrollo de su actividad principal.		
ISO 27.002 11.1.3 y 11.2.1 [14]		

IS1.1.21	Nivel B	F
Proceso de implementación de áreas restringidas		
La organización deberá clasificar como áreas restringidas a aquellas áreas que manejen, almacenen o gestionen información clasificada con sensibilidad MEDIA. Dichas áreas de seguridad deberán implementar todos los lineamientos establecidos para las áreas restringidas,		
ISO 27.002 11.1.3 y 11.2.1 [14]		

IS1 CONTROLES GENERALES DE SEGURIDAD

IS1.2 Uso de Activos de Información

Objetivo Establecer los fundamentos de seguridad relativos al uso de los activos de información por parte de los recursos humanos y usuarios (tanto propios como de terceras partes) vinculados a la organización.

IS1.2.1	Nivel E	F
Subproceso de gestión del uso de activos		
Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados a la información y a las instalaciones de procesamiento de la información. *Se recomienda el establecimiento de una política de uso aceptable de activos de la organización.*		
ISO 27.001 A.8.1.3 [1]		

IS1.2.2	Nivel E	F
Subproceso de gestión del uso de activos		
Todos los usuarios (tanto empleados, contratados, consultores, contratistas y usuarios de terceras partes) deberán devolver todos los activos de la organización en su poder tras la terminación de su empleo, contrato o acuerdo.		
ISO 27.001 A.8.1.4 [1]		

IS1.2.3	Nivel E	F
Subproceso de gestión del uso de activos		
La organización deberá asegurar que no se retire de sus instalaciones: a) Equipamiento (incluyendo hardware y otros dispositivos y activos propiedad o bajo custodia de la organización). b) Información vinculada a la organización (generada, almacenada, en custodia o transmitida hacia/desde la organización). c) Cualquier tipo de software utilizado o desarrollado por la organización. Para una satisfactoria implementación del presente apartado, la organización deberá: d) Identificar a los usuarios, tanto empleados como de terceras partes, que tienen autoridad para permitir el retiro de los activos fuera de la organización. e) Establecer límites de tiempo para el retiro del equipamiento y verificar el cumplimiento de su devolución. f) Registrar cuándo se retira el equipamiento de la organización y cuándo se lo devuelve. Se deberá realizar un registro electrónico en todos los casos. Para el retiro o devolución de terceras partes, se deberá a su vez realizar un registro escrito. g) Documentar la identidad, el rol y la afiliación de cualquier persona que utilice activos de la organización (tanto sean o no propiedad de esta).		
ISO 27.001 A.11.2.5 [1] – ISO 27.002 11.2.5 [14]		

IS1.2.4	Nivel D	F
Subproceso de gestión del uso de activos		
En función de IS1.2.1, los usuarios (tanto empleados, contratados, consultores, contratistas y usuarios de terceras partes) que usen o tengan acceso a los activos de información de la organización deberán: a) Ser conscientes de los requerimientos de SI asociados a los activos de información, recursos y facilidades de procesamiento de información de la organización, b) Ser responsables por su uso de cualquier tipo de recurso de procesamiento de información y activo de información de la organización. Deberán rendir cuentas por dicho uso ante la organización. Se deberá establecer una política de uso aceptable de activos de la organización.		
ISO 27.002 8.1.3 [14]		

IS1.2.5	Nivel D	F
Subproceso de gestión del uso de activos		
La organización deberá establecer una política de escritorios (físicos y digitales) limpios. La misma es conocida generalmente como “política de pantallas y escritorios limpios”. Los medios removibles se encuentran alcanzados dentro de esta política. La política de escritorios limpios deberá tener en cuenta los siguientes lineamientos: a) Deberá considerar las clasificaciones de la información, los requerimientos legales, regulatorios, estatutarios y contractuales y los correspondientes riesgos y aspectos culturales de la organización. b) Se deberá almacenar bajo llave la información clasificada independientemente del tipo de medio en la que se almacene (por ejemplo, en papel o en un medio de almacenamiento electrónico) cuando no se la utilice, especialmente cuando la oficina está desocupada. La información clasificada con sensibilidad CRITICA y ALTA podrá únicamente almacenarse en medios digitales con triple o doble		

cifrado respectivamente (el proceso de cifrado de información deberá realizarse en función de lo establecido en el Domino de Seguridad IS2.1) o dentro de cajas fuertes de alta seguridad si la información se encontrara en soporte físico. La información clasificada con sensibilidad MEDIA deberá ser almacenada digitalmente con al menos un nivel de cifrado o en una cajas fuertes o gabinetes u otras formas de mobiliario seguro de encontrarse en formato físico.
c) Se debe cerrar la sesión de las computadoras y las terminales o protegerlas con un mecanismo de bloqueo de pantalla y teclado controlado por contraseña, dispositivo o mecanismo similar de autenticación de usuario cuando se las deje desatendidas, y su protección mediante cerraduras o candados, contraseñas u otros controles cuando no estén en uso.
c) Se debe prevenir el uso no autorizado de fotocopiadoras y otras tecnologías de reproducción (por ejemplo, escáner, cámaras digitales, cámaras de dispositivos móviles, entre otros).
d) Se debe retirar inmediatamente de las impresoras los documentos que contengan información sensible o clasificada.

ISO 27.001 A.11.2.9 [1] - ISO 27.002 11.2.9 [14]

IS1.2.6	Nivel D	F

Subproceso de gestión del uso de activos

Se deberá diseñar, establecer, mejorar, mantener y documentar los procesos de:

a) Asignación o alta de activos.
b) Desvinculación de activo.
c) Modificaciones de activos.

Por activos, el presente requerimiento hace referencia a todos los activos físicos y electrónicos previamente entregados, que sean propiedad de o le hayan sido confiados a la organización.

Se debe tener especial atención en los casos en los que el usuario (tanto empleados, contratados, consultores, contratistas y usuarios de terceras partes) compren equipamiento de la organización o utilicen el suyo propio. Se deberá diseñar e implementar procesos y controles que aseguren que toda la información se transfiera a la organización y se elimine de manera segura del equipamiento.

ISO 27.002 8.1.4 [14]

IS1.2.7	Nivel D	F
Subproceso de gestión de medios removibles		
Se deben implementar procesos para la gestión de medios removibles en función del esquema de clasificación de la información adoptado por la organización (establecido en función de LS2.3.6). Se deberán considerar los siguientes lineamientos por parte de la organización: a) Los contenidos del medio removible deberán ser irrecuperables, en el caso que este ya no sea requerido por la organización. b) Se deberá llevar un registro de la eliminación de los medios removibles. c) Se deberá almacenar todos los medios removibles en un entorno seguro y protegido, de acuerdo con las especificaciones de los fabricantes. d) Gestionar el inventario de medio removibles con el objetivo de mitigar el riesgo de degradación de los medios cuando los datos almacenados siguen siendo necesarios para la organización. Permitiendo así transferir los datos a un nuevo medio antes de que el original se vuelva ilegible. e) Se deberá almacenar múltiples copias de datos de valor en medios separados para reducir aún más el riesgo de daño o pérdida simultáneos. f) Establecer un registro o base de datos de medios removibles para limitar la oportunidad de perdida de datos y medio removibles. *Se recomienda utilizar técnicas criptográficas para proteger los datos e información almacenada en los medios removibles.*		
LS2.3.6		
ISO 27.001 A.8.3.1 [1] - ISO 27.002 8.3.1 [14]		

IS1.2.8	Nivel D	F
Subproceso de gestión de medios removibles		
La organización deberá establecer procesos formales que aseguren que una vez que los medios de almacenamiento dejen de ser requeridos, estos sean eliminados en forma segura.		

Los procesos para la disposición final segura de los medios que contengan información confidencial deberán ser proporcionales a la sensibilidad de esa información.

Se deberán considerar los siguientes lineamientos para la implementación del presente requerimiento:

a) establecer procedimientos para identificar los ítems que pueden requerir disposición final segura.
b) Consolidar la gestión de todos los medios, en lugar de hacerlo en forma separada o aislada.
c) En el caso que la organización tenga la intención de contratar a organizaciones que ofrecen servicios de recolección y disposición final de medios, se recomienda seleccionar cuidadosamente a una tercera parte apta que cuente con los controles y la experiencia adecuados.
d) Asegurar que los medios que contengan información confidencial se almacenen y eliminen de manera segura, por ejemplo: incinerándolos o triturándolos o borrando los datos (de forma segura, utilizando al menos 1 barrido de sobre escritura de datos) para evitar su uso por otra aplicación.
e) Realizar un análisis de riesgos para determinar si es recomendable destruir los medios removibles en lugar de enviarlos a reparar o desecharlos.

ISO 27.001 A.8.3.2 [1] - ISO 27.002 8.3.2 [14]

IS1.2.9	Nivel D	F

Subproceso de gestión del uso de activos

La organización debe asegurarse que los usuarios (tanto empleados, contratistas como de terceras partes) no dejen equipamiento desatendido sin la protección adecuada.

La organización deberá concientizar a todos los usuarios acerca de los requisitos y procedimientos de seguridad para la protección del equipamiento desatendido, como así también de sus responsabilidades para la implementación de dicha protección. Los usuarios siempre deberán:

a) Finalizar las sesiones activas cuando hayan finalizado sus tareas, a menos que se puedan asegurar con un mecanismo adecuado de bloqueo (por ejemplo: un protector de pantalla protegido por contraseña).
b) Cerrar su sesión en aplicaciones o servicios de red cuando ya no sean necesarios.
c) Proteger sus computadoras o dispositivos móviles del uso no autorizado mediante una traba que necesite de una clave o llave o un control equivalente, cuando no estén en uso. Los dispositivos móviles deberán utilizar una contraseña de caracteres y números en detrimento de la implementación de patrones o PIN de desbloqueo.

ISO 27.001 A.11.2.8 [1] - ISO 27.002 11.2.8 [14]

IS1.2.10	Nivel C	F

Subproceso de gestión del uso de activos

Los medios que contengan información deben encontrarse protegidos contra accesos no autorizados, mal uso o corrupción durante el transporte.

Para proteger la información dentro de medios que sean transportados, la organización deberá:

a) Utilizar medios de transporte o servicios de mensajería confiables.
b) Establecer, por parte de la dirección ejecutiva, una lista de servicios de mensajería autorizados.
c) Desarrollar procedimientos para la verificación de la identificación de los servicios de mensajería.
d) Asegurarse que el embalaje sea suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito y de acuerdo con las especificaciones de cualquier fabricante (por ejemplo, la exposición al calor, la humedad o campos electromagnéticos).
e) Llevar registros que identifiquen el contenido de los medios, la protección aplicada y de los tiempos de transferencia a los custodios durante el traslado y de la recepción en el destino.
f) Cifrar toda la información contenida dentro de medios. En el caso de no ser posible o dificultoso (por ejemplo, documentos en papel), establecer una protección física adicional para los medios.

ISO 27.001 A.8.3.3 [1] - ISO 27.002 8.3.3 [14]

IS1.2.11	Nivel C	F
Subproceso de gestión de medios removibles		
Se deberán considerar los siguientes lineamientos por parte de la organización para la gestión de medios removibles: a) Previo a la eliminación, se deberá contar con una autorización por parte del RAI o RAIs responsables de la información contenida dentro del medio removible. b) Se deberán utilizar técnicas criptográficas para proteger los datos e información almacenada en los medios removibles. c) Cuando sea necesario utilizar medios removibles, monitorear la transferencia de información a los medios removibles. d) Las unidades de medios removibles sólo deberán encontrarse activas siempre y cuando exista una razón de negocio que sustente su uso. e) Se deberán documentar los procesos y niveles de autorización vinculados a la gestión de medios removibles. f) Se deberá registrar y documentar la disposición final de ítems sensibles de la organización para mantener evidencias de auditoría. g) Al momento de eliminar de forma segura un medio removible, deberá borrarse sus datos de forma segura, utilizando al menos 3 barridos de sobre escritura de datos.		
ISO 27.002 8.3.1 y 8.3.2 [14]		

IS1.2.12	Nivel C	F
Subproceso de gestión del uso de activos		
La organización deberá realizar verificaciones al azar para: a) Detectar el retiro no autorizado de activos. b) Detectar dispositivos de grabación no autorizados, armas u otros dispositivos prohibidos por la organización (establecidos dentro de la política de gestión d Activos de información). c) Prevenir la entrada y salida de los activos de las instalaciones.		

Las verificaciones al azar deberán llevarse a cabo de acuerdo con la legislación y las regulaciones pertinentes. Las personas (empleados, contratistas y terceras partes vinculadas a la organización) deben estar al tanto de que se llevarán a cabo verificaciones al azar.

Las verificaciones solo se deben realizar con autorización apropiada según los requisitos legales y regulatorios correspondientes.

ISO 27.002 11.2.5 [14]

IS1.2.13	Nivel C	F

Subproceso de gestión del uso de activos

Se deberá aplicar seguridad a los activos que se encontrarán fuera de la organización teniendo en cuenta los diferentes de trasladarlos y utilizarlos fuera de las instalaciones de la organización. El uso de cualquier activo de la organización fuera de sus instalaciones deberá ser autorizado por la dirección ejecutiva. Esto último aplica al equipamiento perteneciente o no a la organización, siempre que se lo utilice para llevar adelante actividades de dicha organización.

Para la protección del equipamiento que se encuentra fuera de la organización, se deberán cumplir los siguientes lineamientos:

a) El equipamiento y los dispositivos retirados de la organización no deberán permanecer desatendidos en lugares públicos.
b) Se deberá siempre respetar las indicaciones del fabricante para la protección del equipamiento.
c) Cuando el equipamiento fuera de la oficina se transfiera entre distintos individuos o terceras partes, se deberá mantener un registro que defina la cadena de custodia para el equipamiento que incluya, como mínimo, los nombres y las organizaciones de aquellos responsables por éste y las fechas de cambio de custodia.
d) Establecer controles y lineamientos a las ubicaciones fuera de las instalaciones de la organización.

ISO 27.001 A.11.2.6 [1] - ISO 27.002 11.2.6 [14]

IS1.2.14	Nivel C	F
Subproceso de gestión del uso de activos		
La organización deberá verificar todos los componentes del equipamiento que contengan medios de almacenamiento para asegurar que, antes de su disposición final o reutilización, se haya eliminado o sobrescrito de manera segura, cualquier dato sensible y software licenciado. Los medios de almacenamiento que contengan información confidencial o con derechos de autor deben destruirse, eliminarse o sobrescribirse usando técnicas que hagan irrecuperable la información original en lugar de utilizar la forma normal de eliminación o la función de formateo (en función de IS1.2.11 o IS1.2.17). Se debe realizar una evaluación de riesgos previamente a enviar un equipamiento para su reparación o descarte, ya que puede contener medios de almacenamiento con información sensible que puede verse comprometida si no se tiene cuidado en la disposición final o la reutilización del equipamiento. La organización deberá asegurarse que todos los medios de almacenamiento que contengan información clasificada como CRITICA y ALTA se encuentren cifrados en forma completa y cumpliendo con todos los siguientes requerimientos: a) El proceso de cifrado debe ser lo suficientemente robusto y cubrir todo el disco en su totalidad (incluyendo su "*slack space*[45]"). b) Las claves de cifrado deben ser lo suficientemente largas como para resistir ataques por fuerza bruta. c) Las claves de cifrado deben mantenerse confidenciales y no deberán almacenarse dentro del mismo disco. A su vez, las claves no deberán ser almacenadas en texto plano.		

ISO 27.001 A.11.2.7 [1] - ISO 27.002 11.2.7 [14]

[45] Espacio no utilizado de un clúster del disco.

IS1.2.15	Nivel C	F
Subproceso de gestión del uso de activos		
La organización deberá únicamente utilizar impresoras con código numérico de identificación personal, de modo que sólo los usuarios que originan el pedido de impresión puedan obtener sus salidas impresas, y solamente cuando se encuentren al lado de la impresora. El uso de teléfonos fijos (IP o similares) debe gestionarse de forma similar.		
ISO 27.002 11.2.9 [14]		

IS1.2.16	Nivel B	F
Subproceso de gestión del uso de activos		
En los casos en que un usuario (tanto empleados, contratados, consultores, contratistas y usuarios de terceras partes) posea conocimientos que sean importantes para el cumplimiento de los objetivos estratégicos de la organización, se deberá documentar y transferir esa información a la organización. La organización deberá controlar las acciones del usuario desde el momento de aviso de la desvinculación, pues podrá aprovechar para realizar copias no autorizadas de la información de la organización. Es por este motivo, que se recomienda el recupero de todos los activos y la baja de todos los privilegios de acceso del usuario antes o al momento de comunicación de su desvinculación. *Se recomienda el uso e implementación de sistemas de bibliotecas de conocimiento.*		
ISO 27.002 8.1.4 [14]		

IS1.2.17	Nivel B	F
Subproceso de gestión de medios removibles		
La organización deberá asegurarse que los medios que contengan información confidencial se almacenen y eliminen de manera segura siguiendo alguno de los siguientes lineamientos: a) incineración. b) trituración. c) Borrando los datos de forma segura, utilizando al menos 7 barridos de sobre escritura de datos. La organización deberá realizar primero la opción c) y luego una de las opciones a) o b), con excepción de aquellos medios removibles que solo contengan información de sensibilidad baja. *Cuando se acumulen medios para su disposición final, la organización deberá considerar el efecto agregación, el cual puede causar que una gran cantidad de información no sensible se vuelva sensible.*		
ISO 27.002 8.3.2 [14]		

IS1.2.18	Nivel B	F
Subproceso de gestión de medios removibles		
La organización deberá asegurarse que todos los medios de almacenamiento que contengan información clasificada como CRITICA, ALTA y MEDIA se encuentren cifrados en forma completa y cumpliendo con todos los requerimientos detallados en		
ISO 27.002 11.2.7 [14]		

IS1 CONTROLES GENERALES DE SEGURIDAD

IS1.3 Gestión de accesos

Objetivo Establecer los fundamentos de la gestión de accesos, credenciales y privilegios a los activos de información de una organización. Enfocándose principalmente en el proceso de asignación, mantenimiento, revisión y remoción de los accesos.

IS1.3.1	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá gestionar la identidad de todos los usuarios que poseen accesos o privilegios de acceso (lectura, escritura, etc.) sobre los activos de información de la organización.		

IS1.3.2	Nivel D	F

Macroproceso de gestión de accesos a activos de información

Se debe establecer, documentar y revisar una política de gestión de accesos basada en los requerimientos del negocio y de la SI de la organización.

La política de gestión de accesos deberá tener en cuenta lo siguiente:

a) Los requerimientos de seguridad de las aplicaciones de negocio (software).
b) El principio de necesidad de saber ("*need to know basis*"[46]) aplicado a la diseminación de información y autorización de acceso a activos de información de la organización.
c) La coherencia entre la política de gestión de accesos y el mecanismo de clasificación de la información de los sistemas y las redes de la organización.
d) La legislación pertinente y cualquier obligación contractual con respecto a la limitación del acceso a datos o servicios.
e) La segregación de los roles de control de acceso (por ejemplo: la solicitud de acceso, la autorización de acceso y la administración de acceso).
f) Los requisitos de autorización formal de las solicitudes de acceso.
g) Los requisitos y lineamientos para las revisiones periódica de los derechos de acceso.
h) Los lineamientos y el proceso para la remoción de los derechos de acceso.
i) El archivo de los registros de todos los eventos significativos respecto del uso y gestión de identidades de los usuarios y la información secreta de autenticación.
j) La gestión de los roles con accesos privilegiado.

La política deberá a su vez, especificar las reglas de control de acceso, teniendo en cuenta que:

k) Deberán establecerse basadas en la premisa "*Todo está prohibido a menos que esté explícitamente permitido*", antes que en la regla más débil "*En general todo está permitido a menos que esté explícitamente prohibido*".
l) El establecimiento de un mecanismo de diseño, aprobación, implementación y mejora de las reglas de control de acceso.
m) Las reglas deberán estar soportadas por políticas, procesos formales y responsabilidades definidas.
n) Los principios de necesidad de saber (solo se le da acceso a la información que necesita para realizar sus tareas) y necesidad de uso (solo se le da acceso a las

[46] Necesidad de saber, traducción del idioma inglés.

instalaciones de procesamiento de información que necesita para realizar su tarea o trabajo).
ISO 27.001 A.9.1.1 [1] - ISO 27.002 9.1.1 [14]

IS1.3.3	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá implementar un proceso formal de alta y baja de registros de usuarios para permitir la asignación de derechos de acceso a los activos de información. Para lo cual la organización deberá establecer un proceso de gestión de identificadores de usuario (altas, bajas, suspensión y activación). Dicho proceso deberá tener en cuenta los siguientes lineamientos: a) El uso de un identificador único que permita a los usuarios estar relacionados y ser responsables de sus propias acciones. No se debe permitir el uso de identificadores de usuario compartidos. Los identificadores de usuario pueden ser denominados de forma tal que no revelen la identidad del usuario que lo utiliza. No obstante, la organización deberá llevar un registro cifrado que vincule a cada usuario (empleado, contratista o tercera parte) con cada identificador de usuario. b) La inhabilitación inmediata o eliminación de los identificadores de usuario de los usuarios que han dejado la organización. c) La identificación periódica y la eliminación o inhabilitación de identificadores de usuario redundantes. d) El aseguramiento de que los identificadores de usuario redundantes no se emitan a otros usuarios. e) El alcance del proceso deberá abarcar tanto la asignación y habilitación, o la revocación de un identificador de usuario como la asignación o revocación de los derechos de acceso para dicho identificador de usuario (vinculado al requerimiento IS1.3.3.		
IS1.3.3		
ISO 27.001 A.9.2.1 [1] - ISO 27.002 9.2.1 [14]		

IS1.3.4	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización debe implementar un proceso formal para otorgar o revocar los derechos de todos los tipos de usuario a todos los sistemas y servicios. Dicho proceso deberá tener en cuenta los siguientes lineamientos: a) Se debe obtener autorización previa para el uso del sistema o servicio de información por parte del responsable del sistema o servicio de información (en estadios de madurez "C" y superiores el responsable será el RAI a cargo del sistema o servicio). b) Se debe verificar que el nivel de acceso otorgado sea apropiado a las políticas de acceso y coherente con otros requisitos como la segregación de tareas. c) Asegurar que los derechos de acceso no se activen (por ejemplo, por proveedores de servicio) antes de completar los procedimientos de autorización. d) Mantener un registro central de todos los derechos de acceso otorgados a un identificador de usuario para acceder a los sistemas y servicios de información. e) Adaptar los derechos de acceso de usuarios que han cambiado de rol o cargo y remover o bloquear inmediatamente los derechos de acceso de usuarios que han dejado la organización (corresponderá suspender si es temporalmente y bloquear si es en forma permanente). f) Revisar en forma periódica los derechos de acceso con los responsables de los sistemas o servicios de información (en estadios de madurez C y superiores el responsable será el RAI a cargo de los sistemas o servicios).		
ISO 27.001 A.9.2.2 [1] - ISO 27.002 9.2.2 [14]		

IS1.3.5	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá controlar la asignación de información secreta de autenticación a través de un proceso formal de gestión. Dicho proceso deberá hacer realidad los siguientes lineamientos: a) Requerir a los usuarios que firmen una declaración por la cual se comprometen a mantener confidencial su información secreta de autenticación individual. Dicha		

declaración firmada debe incluirse en los términos y condiciones del empleo o contrato.
b) Entregar inicialmente una información secreta de autenticación provisoria que estén obligados a modificar en el primer uso.
c) Establecer procedimientos para verificar la identidad de un usuario antes de proveerle información secreta de autenticación nueva, de reemplazo o provisoria.
d) Entregar a los usuarios la información secreta de autenticación provisoria de manera segura, evitando el uso de terceras partes o medios no protegidos (por ejemplo: correo electrónico no cifrado).
e) Que la información secreta de autenticación provisoria sea única para una persona.
f) Que la información secreta de autenticación provisoria no sea adivinable (es decir, que no siga una secuencia o patrón, variando así en forma permanente).
f) Que los usuarios confirmen la recepción de la información secreta de autenticación y que se guarde registro de ello.
g) Cambiar la información secreta de autenticación predeterminada que otorga el vendedor luego de la instalación de del software o hardware.

A su vez, la organización deberá:

h) Revisar periódicamente los derechos de acceso de todo tipo de usuarios a intervalos regulares y después de cualquier cambio (desvinculación, suspensión, renuncia, cambio de rol, puesto o área, rescisión del contrato, entre otros).
i) Revisar a intervalos más cortos las autorizaciones para los derechos de acceso privilegiado.
k) Verificar las asignaciones de privilegios a intervalos regulares para asegurar que no se han obtenido privilegios no autorizado.

ISO 27.001 A.9.2.4 [1] - ISO 27.002 9.2.4 y 9.2.5 [14]

IS1.3.6	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá restringir el acceso a la información y a las funciones de los sistemas de aplicaciones en función de los lineamientos establecidos por la política de gestión de accesos de la organización (establecida en IS1.3.1).		

La restricción de acceso deberá basarse en los requisitos individuales de negocio para cada aplicación, servicio o sistema y en las autorizaciones y lineamientos para la gestión de los accesos establecidos en la política de gestión de accesos de la organización (establecida en IS1.3.1).
IS1.3.1
ISO 27.001 A.9.4.1 [1] - ISO 27.002 9.4.1 [14]

IS1.3.7	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
Las contraseñas no podrán ser transmitidas en texto plano en ningún momento de su ciclo de vida. A su vez, tampoco podrán ser almacenadas en texto plano.		
ISO 27.002 9.4.2 [14]		

IS1.3.8	Nivel D	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá diseñar, implementar y mantener actualizada al día una matriz de recursos de información y sus correspondientes accesos otorgados. *Se recomienda la implementación de un sistema automatizado para la gestión de dichos registros y accesos como así también la implementación de alguna metodología de "Single sing-on".*		

IS1.3.9	Nivel C	F
Macroproceso de gestión de accesos a activos de información		
La organización deberá cumplir con los siguientes lineamientos de gestión de accesos a la información:		

a) Limitar la información contenida en las salidas a lo necesario para desarrollar las actividades de negocio correspondientes.
b) Controlar los derechos de acceso de todas las aplicaciones, servicios y sistemas de la organización. De ser posible, mantenerlos actualizados en forma automática.
c) Controlar los derechos de acceso (lectura, escritura, eliminación y ejecución) de todos los usuarios (propios, contratistas y de terceras partes) en función de los lineamientos de gestión de accesos establecidos en IS1.3.1 y IS1.3.5.
d) Controlar los datos a los que puede acceder un usuario (propio, contratistas y de terceras partes) en particular.
e) Proveer menús para controlar el acceso a las funciones de los sistemas de aplicaciones.
f) Proveer controles de acceso físico o lógico, a fin de aislar las aplicaciones, datos de aplicaciones o sistemas sensibles.

IS1.3.1
ISO 27.002 9.4.1 [14]

IS1.3.10	Nivel C	F

La organización debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado a través de un proceso formal de autorización, en función de la política de gestión de accesos de la organización.

El proceso deberá tener en cuenta los siguientes lineamientos:

a) Identificar y registrar los derechos de acceso privilegiado asociados a cada sistema o proceso y cada aplicación y los usuarios a quienes se los necesita asignar.
b) Asignar los derechos de acceso privilegiado en base a la necesidad de uso y evento por evento, en línea con la política de gestión de accesos, teniendo en cuenta el requisito mínimo para los roles funcionales de las personas y contando con la debida aprobación del RAI o RAIs correspondientes.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. No se debe otorgar los derechos de acceso privilegiado hasta que se haya completado el proceso de autorización. Ante emergencias, la organización

deberá establecer un proceso de autorización rápida de emergencia para el uso de los derechos de acceso privilegiado.
d) Definir los requisitos para la expiración de los derechos de acceso privilegiado.
e) Asignar los derechos de acceso privilegiado a un identificador de usuario diferente de aquellos identificadores utilizados en las actividades usuales del negocio. Las actividades usuales del negocio no deben realizarse utilizando identificadores privilegiados.
f) Revisar periódicamente las competencias de los usuarios con derechos de acceso privilegiado con el fin de verificar si están alineadas con sus tareas y sus autorizaciones correspondientes.
g) Establecer y mantener procedimientos específicos con el fin de evitar el uso no autorizado de identificadores de usuario administrador genérico, de acuerdo con las opciones de configuración de los sistemas.
h) Mantener la confidencialidad de la información secreta para la autenticación cuando se la comparte. Por lo que se deberá cambiar las contraseñas frecuentemente y lo antes posible ante la renuncia, suspensión, despido o cambio de trabajo/rol de un usuario privilegiado. A su vez, las contraseñas deberán ser comunicadas a través de medios seguros cifrados.
i) Llevar un registro de los cambios a las cuentas con privilegios para revisarlas periódicamente.

ISO 27.001 A.9.2.3 [1] - ISO 27.002 9.2.3 y 9.2.5 [14]

IS1.3.11	Nivel C	K

Macroproceso de gestión de accesos a activos de información

Los derechos de acceso tanto lógicos como físicos a la información y a las instalaciones de procesamiento de información de todos los usuarios (tanto sean empleados, contratistas o de terceras partes) deben:

a) Ser eliminados tras la finalización de su empleo, contrato o acuerdo (incluyendo renuncia y despido).
b) Ser ajustados (modificados) a cualquier cambio en sus tareas, rol, puesto o área de trabajo. Siempre en función del principio de necesidad de saber ("*need to know basis*[47]") y necesidad de uso, establecidos en IS1.3.1.n. Se requerirá la eliminación de todos los derechos de acceso que no hayan sido aprobados o necesarios para

[47] Necesidad de saber, traducción del idioma inglés.

el desempeño de su nuevo rol. Los accesos deberán ser modificados antes de efectivizarse el cambio en las tareas, rol, puesto o área de trabajo.
c) Ser suspendidos durante cualquier tipo de licencia (vacaciones, días de enfermedad, licencia sin goce de sueldo, entre otras) o suspensión (en este caso deberán ser suspendidos inmediatamente, hasta que el o los RAIs correspondientes tomen la decisión de eliminar o no los derechos de acceso).

En caso de despido, todos los accesos deberán ser eliminados previo a informar la recisión del contrato al empleado, contratista o tercera parte.

En caso de renuncia, los accesos que permitan manipular información clasificada como CRÍTICA o ALTA deberán ser eliminados inmediatamente. Para el resto de los accesos, cada RAI decidirá si los mantiene activos y hasta que momento. No obstante, para el día de la fecha efectiva de renuncia, todos los accesos deberán haber sido eliminados.

A su vez, la organización deberá:

a) Modificar cualquier documentación que identifique los derechos de acceso de empleados, contratistas y usuarios de terceras partes, ya que deberá reflejar la remoción o el ajuste de los derechos de acceso.
b) Modificar las contraseñas para todos los identificadores que permanecen activos y hayan sido vinculados a un usuario, contratista o tercera parte, al momento de su renuncia, despido, suspensión, recisión de contrato o cambio de puesto, contrato o acuerdo.

IS1.3.1.n
ISO 27.001 A.9.2.6 [1] - ISO 27.002 9.2.6 [14]

IS1.3.12	Nivel C	F
Macroproceso de gestión de accesos a activos de información		
Cada RAI individual será responsable (y rendirá cuentas) por el diseño, implementación, mantenimiento y mejora de los procesos establecidos en IS1.3.2 y IS1.3.3 de los activos de información bajo su responsabilidad. Cada RAI será a su vez responsable por que los activos de información a su cargo sean gestionados, utilizados, almacenados, mantenidos y, eventualmente,		

desechados en forma segura y en función de los lineamientos establecidos por la política de gestión de accesos de la organización (referirse a IS1.3.1).

Los RAI serán responsables de:

a) Determinar las reglas de control de accesos, los derechos y las restricciones para roles de usuarios específicos con respecto a los activos de información a su cargo. El diseño de los roles deberá realizarse con un nivel de detalle y rigurosidad de controles que refleje el análisis de los riesgos asociados al activo respecto de la SI.

Los controles detallados en a) deberán ser tanto lógicos como físicos.

Podrá encontrarse mayor detalle sobre las responsabilidades de los RAI dentro del requerimiento LS2.1.6.

ISO 27.002 9.1.1 [14]

IS1.3.13	Nivel C	F

Macroproceso de gestión de accesos a activos de información

La organización deberá controlar el acceso a los sistemas, servicios y aplicaciones mediante un proceso formal de inicio de sesión, cuando lo requiera la política de gestión de accesos.

Se deberán seleccionar diferentes técnicas de autenticación para corroborar la identidad declarada por el usuario. Para el acceso a la información clasificada con sensibilidad CRÍTICA deberá requerirse, adicionalmente al uso de una contraseña, el uso de al menos 1 método de autenticación fuerte (medios criptográficos, tarjetas inteligentes, tokens o dispositivos biométricos).

A su vez, la organización deberá diseñar un proceso de inicio de sesión que cumpla con los siguientes lineamientos de seguridad:

a) El inicio de sesión de un sistema o aplicación debe encontrarse diseñado para minimizar la oportunidad de acceso no autorizado.

b) No se deberán mostrar identificadores del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado exitosamente.
c) Mostrar una advertencia general de notificación indicando que a la computadora sólo acceden usuarios autorizados.
d) No proveer mensajes de ayuda durante el procedimiento de inicio de sesión que puedan ayudar a un usuario no autorizado.
d) Validar la información de inicio de sesión solamente luego de haberse completado el ingreso de todos los datos. Si aparece una condición de error, se recomienda que el sistema no indique qué parte de los datos es correcta o incorrecta.
e) Proteger contra los intentos de iniciar una sesión empleando fuerza bruta;
f) Registrar los intentos exitosos y fallidos.
g) Iniciar un evento de seguridad cuando detecte un intento potencial o una violación exitosa de los controles de inicio de sesión.
h) Al completarse un inicio de sesión exitoso, muestre la siguiente información:

- fecha y hora del inicio de sesión exitoso anterior.
- detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso.

i) No mostrar la contraseña ingresada.
j) No transmitir contraseñas en formato de texto plano a través de una red.
k) Cerrar sesiones luego de un período definido de inactividad, especialmente en ubicaciones de alto riesgo como áreas públicas o externas a la gestión de la seguridad de la organización o en dispositivos móviles.
l) Limitar el tiempo de conexión para proveer de seguridad adicional a las aplicaciones de alto riesgo y reducir la ventana de oportunidad de accesos no autorizados.

ISO 27.001 A.9.4.2 [1] - ISO 27.002 9.4.2 [14]

IS1.3.14	Nivel C	F

Macroproceso de gestión de accesos a activos de información

La organización deberá controlar adecuadamente el uso de utilitarios con privilegios. Deberá restringir y controlar rigurosamente el uso de herramientas que podrían ser capaces de pasar por alto los controles del sistema o de las aplicaciones.

Para el uso de estas herramientas la organización deberá: a) Utilizar procedimientos de identificación, autenticación y autorización para las herramientas. b) Segregar las herramientas del software de las aplicaciones. c) Limitar el uso de herramientas al mínimo número práctico de usuarios de confianza autorizados. d) Autorizar el uso "ad hoc" de las herramientas. e) Limitar la disponibilidad de las herramientas, por ejemplo, durante un cambio autorizado. f) Registrar todo uso de las herramientas. g) Definir y documentar los niveles de autorización para las herramientas. h) Remover o desactivar todas las herramientas innecesarias. i) No dejar disponibles las herramientas a usuarios que tienen acceso a aplicaciones en sistemas en los que se requiera la segregación de tareas.
ISO 27.001 A.9.4.4 [1] - ISO ISO 27.002 9.4.4 [14]

IS1.3.15	Nivel C	K
Macroproceso de gestión de accesos a activos de información		
La organización deberá implementar alguna solución de "*Identity management*" para la gestión de accesos a sus activos de información. Dicha solución deberá basarse en la metodología "*single sing-on*".		

IS1.3.16	Nivel B	F
Macroproceso de gestión de accesos a activos de información		
Para el acceso a la información clasificada con sensibilidad ALTA o CRÍTICA se requerirá, adicionalmente al uso de una contraseña, el uso de al menos 2 métodos de autenticación fuertes (medios criptográficos, tarjetas inteligentes, tokens o dispositivos biométricos).		

Para el acceso a la información clasificada con sensibilidad MEDIA deberá requerirse, adicionalmente al uso de una contraseña el uso de al menos 1 método de autenticación fuerte.

[Página dejada en blanco intencionalmente]

IS2 PROTECCIÓN Y DEFENSA DE LA SEGURIDAD

IS2.1 Protección de la Información

Objetivo Establecer los fundamentos de seguridad que permitirán establecer barreras de seguridad para la protección de la información de la organización y asegurara su confidencialidad, disponibilidad e integridad.

IS2.1.1	Nivel E	F
Macroproceso de protección de la información		
La organización deberá producir, conservar y revisar periódicamente los registros de eventos en los cuales se registren las actividades de los usuarios, las excepciones, los errores y los eventos de SI. Los registros de eventos deberán incluir: a) Los identificadores de usuarios. b) Las actividades del sistema. c) Las fechas, los horarios y los detalles de los eventos principales (por ejemplo: inicio y cierre de sesión). d) Los registros de intentos exitosos y rechazados del acceso al sistema. e) El uso de privilegios. f) Las alarmas ejecutadas por el sistema de control de acceso.		

ISO 27.001 A.12.4.1 [1] - ISO 27.002 12.4.1 [14]

IS2.1.2	Nivel E	F
Macroproceso de protección de la información		
La organización deberá llevar un registro de todas las actividades de los administradores y operadores de sistemas, debiendo estos registros encontrarse permanentemente protegidos (contra manipulación, adulteración, indisponibilidad o acceso no autorizado). Dichos registros deberán ser revisados periódicamente.		
ISO 27.001 A.12.4.3 [1] - ISO 27.002 12.4.3 [14]		

IS2.1.3	Nivel E	F
Macroproceso de protección de la información		
Todos los relojes de todos los sistemas vinculados a la organización deberán encontrarse adecuadamente sincronizados de acuerdo a una única fuente de tiempo de referencia. Para lo cual, la organización debe: a) Definir un tiempo de referencia normalizado para utilizar dentro de la organización. b) Documentar e implementar el enfoque de la organización para obtener un tiempo de referencia de una o más fuentes externas y cómo sincronizar los relojes internos de manera confiable. c) Documentar los requisitos externos (legales, reglamentarios o de normativas) e internos (contractuales o de lineamientos internos) para la representación, la sincronización y la exactitud del tiempo.		
ISO 27.001 A.12.4.4 [1] - ISO 27.002 12.4.4 [14]		

IS2.1.4	Nivel E	F
Macroproceso de protección de la información		
La organización deberá establecer políticas, procesos y controles formales para proteger la transferencia de información tanto en formato digital como físico. A su vez, la organización deberá: a) Establecer procesos para la protección de la información electrónica sensible comunicada que se encuentra en forran de adjunto (por ejemplo: a través de la implementación de nubes de archivos cifradas). b) Establecer políticas o lineamientos para el uso aceptable de las instalaciones de comunicaciones. c) Establecer, comunicar y documentar las responsabilidades del usuario (ya sea personal, de tercera parte y cualquier otro) de no comprometer a la organización (por ejemplo: a través de la difamación, el hostigamiento, la suplantación de identidad, el reenvío de cadenas de cartas, las compras no autorizadas, entre otras acciones). d) Asegurarse que los usuarios (empleados, contratistas y de terceras partes) no dejen mensajes que contengan información confidencial en contestadores automáticos debido a que configuran un riesgo de seguridad. e) Advertir al personal acerca de los problemas del uso de equipos o servicios de fax, prohibiendo su uso exceptuando algún caso puntual requerido por la naturaleza del negocio que requiera autorización expresa de los RAIs a cargo de la información a transmitirse. f) Asegurarse que los servicios de transferencia de información que utilice cumplan con los requisitos legales y regulatorios pertinentes.		
ISO 27.001 A.13.2.1 [1] - ISO 27.002 13.2.1 [14]		

IS2.1.5	Nivel D	F
Macroproceso de protección de la información		
La organización deberá identificar y documentar la coordinación y la supervisión de los aspectos de SI en las relaciones con los proveedores.		
ISO 27.002 6.1.1.e [14]		

IS2.1.6	Nivel D	F
Macroproceso de protección de la información		
Se deberán documentar todos los procedimientos operativos y procesos relativos a la SI de la organización. La documentación deberá estar disponible para todos los usurarios que los requieran para el normal desarrollo de sus tareas. Los procedimientos operativos deberán especificar instrucciones operativas, incluyendo: a) La instalación y la configuración de sistemas. b) El procesamiento y la manipulación de la información, tanto automatizada como manual. c) El resguardo. d) La programación de los requisitos, incluyendo las interdependencias con otros sistemas, el tiempo más temprano de inicio de un trabajo y el tiempo más tardío de finalización de un trabajo. e) Las instrucciones para el tratamiento de los errores y otras condiciones excepcionales que puedan surgir durante la ejecución de un trabajo, incluyendo las restricciones sobre el uso de utilitarios. f) Los contactos de soporte y escalamiento, incluyendo contactos de soporte externo en el caso de dificultades operativas o técnicas inesperadas. g) Las instrucciones especiales para las salidas y la manipulación de medios, tales como el uso de papel especial o la gestión de salidas confidenciales incluyendo procedimientos para la disposición segura de las salidas de trabajos fallidos. h) Los procedimientos para el reinicio y la recuperación de los sistemas a utilizar en el caso de fallas. i) La gestión de la información de las trazas para la auditoría y de los registros de los sistemas. j) Los procedimientos de monitoreo. Los cambios a los procedimientos operativos deberán ser adecuadamente documentados y aprobados. Lo mismo será aplicable a los procesos de SI, donde el Responsable del proceso será quien debe aprobar las modificaciones.		
ISO 27.001 A.12.1.1 [1] - ISO 27.002 12.1.1 [14]		

IS2.1.7	Nivel D	F
Macroproceso de protección de la información		
La organización deberá asegurarse de que se realicen copias para el resguardo de toda la información, el software y los sistemas. Las copias de resguardo deberán ser sometidas periódicamente a pruebas para asegurar su confidencialidad, integridad y disponibilidad ante una eventual necesidad de la organización. La generación, almacenamiento, custodia y eliminación de las copias de respaldo deberán ser acordes a los lineamientos de la política de gestión de copias de respaldo de la organización.		
ISO 27.001 A.12.3.1 [1] - ISO 27.002 12.3.1 [14]		

IS2.1.8	Nivel D	F
Macroproceso de protección de la información		
La organización deberá implementar, documentar y mantener una política de gestión de copias de respaldo. La misma deberá: a) Definir los requisitos de la organización para el resguardo de la información, el software y los sistemas. b) Definir los requisitos de retención y protección. c) Establecer los lineamientos a cumplir por la organización para contar con instalaciones de resguardo adecuadas para asegurar que toda la información y el software esenciales puedan ser recuperados luego de un desastre o una falla de medios. d) Asegurar que se generen registros exactos y completos de las copias de resguardo y la correcta documentación de los procesos de restauración. e) Asegurar que las copias de resguardo se almacenen en una ubicación remota, a una distancia suficiente para escapar de cualquier daño producido por un desastre en el sitio principal de la organización. f) Asegurar que se le otorgue a la información de resguardo un adecuado nivel de protección física y del entorno coherente con las normas aplicadas al sitio principal.		

g) Asegurar que se prueben periódicamente los medios de resguardo para asegurar que se puede confiar en ellos en casos de emergencia. A realizarse en combinación con una prueba de los procedimientos de restauración y con la verificación de que se cumpla el tiempo de restauración requerido.
ISO 27.001 A.12.3.1 [1] - ISO 27.002 12.3.1 [14]

IS2.1.9	Nivel D	F
Macroproceso de protección de la información		
La organización deberá asegurarse que tanto la información de registros de eventos como las instalaciones en donde se almacenen y procesen dichos registros sean protegidas contra manipulación, modificación, acceso no autorizado y problemas operativos que podrían dificultar su normal identificación y registro. Se deberán implementar controles que impidan: a) Las alteraciones de los tipos de mensajes que se registran. b) La edición o la eliminación de los archivos de los registros. c) Que se exceda la capacidad de almacenamiento del medio en el cual se archivan los registros, resultando en la incapacidad de registrar los eventos o la sobreescritura de eventos ya registrados previamente.		
ISO 27.001 A.12.4.2 [1] - ISO 27.002 12.4.2 [14]		

IS2.1.10	Nivel D	F
Macroproceso de protección de la información		
Los registros de eventos, adicionalmente a lo estipulado en IS2.1.1, deberán incluir: a) Los registros de intentos exitosos y rechazados de acceso a los datos u otro recurso. b) Los cambios en la configuración del sistema.		

c) El uso de utilitarios y aplicaciones de sistemas. d) Los archivos accedidos y el tipo de acceso. e) Las direcciones de red y los protocolos.
IS2.1.1
ISO 27.002 12.4.1 [14]

IS2.1.11	Nivel D	F
Macroproceso de protección de la información		
En función de la protección y aseguramiento de la transferencia de información, la organización deberá: a) Establecer procesos para proteger la información transferida de la intercepción, copia, modificación, ruteo erróneo y su destrucción. b) Establecer los lineamientos para la retención y la eliminación de toda la correspondencia del negocio, incluyendo los mensajes, de acuerdo con las leyes y regulaciones locales y nacionales pertinentes. c) Diseñar, implementar y mantener controles y restricciones asociados al uso de las instalaciones de comunicaciones (por ejemplo: evitar el reenvío automático de correo electrónico a direcciones externas de correo electrónico).		
ISO 27.002 13.2.1 [14]		

IS2.1.12	Nivel D	F
Macroproceso de protección de la información		
La organización deberá desarrollar, establecer y documentar acuerdos que aborden la transferencia de información del negocio entre la organización y las partes externas. *Se recomienda el desarrollo de una Política de Seguridad conjunta entre la organización y la parte externa que delinee todos los aspectos y lineamientos fundamentales de la SI en la relación entre estas dos organizaciones.*		

ISO 27.001 A.13.2.2 [14] – ISO 27.001 A.15.1.1 [14]

IS2.1.13	Nivel C	F
Macroproceso de protección de la información		
Los registros de eventos, adicionalmente a lo estipulado en IS2.1.1 y IS2.1.9, deberán incluir: a) La identidad del dispositivo o la ubicación si fuera posible y el identificador del sistema. b) La activación y la desactivación de los sistemas de protección, tales como los sistemas antivirus y los sistemas de detección de intrusos. c) Los registros de las transacciones ejecutadas por los usuarios en las aplicaciones. La organización deberá implementar sistemas de seguimiento automatizado de los registros de eventos que sean capaces de generar informes consolidados y alertas en tiempo real sobre la seguridad de los sistemas de la organización. Los registros de eventos deberán estar adecuadamente protegidos. Deberán encontrarse cifrados en su totalidad en concordancia con los lineamientos de controles criptográficos del MRU). A su vez, deberá realizarse una copia en tiempo real de los registros hacia otro sistema que se encuentre fuera del control del administrador u operador del sistema del cual se toman los registros. Los administradores de sistema no deberán tener permiso para borrar o desactivar los registros de sus propias actividades.		
IS2.1.1 - IS2.1.9		
ISO 27.002 12.4.1 [14]		

IS2.1.14	Nivel C	F
Macroproceso de protección de la información		
La política de gestión de copias de respaldo deberá asegurar:		

a) Que la extensión (por ejemplo: resguardo completo o diferencial) y la frecuencia de los resguardos reflejen los requisitos de negocio de la organización, los requisitos de SI involucrada y la criticidad de la información para la continuidad operativa de la organización.
b) Que las copias de resguardo se encuentren cifradas en función de los lineamientos del MRU según la criticidad de cada activo de información.

ISO 27.001 A.12.3.1 [1] - ISO 27.002 12.3.1 [14]

IS2.1.15	Nivel C	F

Macroproceso de protección de la información

La organización deberá desarrollar, implementar y mantener una política de controles criptográficos para la protección de la confidencialidad de la información.

La política de controles criptográficos deberá abordar lo siguiente:

a) El enfoque de gestión (lineamientos y objetivos estratégicos) respecto del uso de controles criptográficos en toda la organización.
b) Identificar, en base a una evaluación de riesgos, el nivel requerido de protección teniendo en cuenta el tipo, la robustez, y la calidad del algoritmo de cifrado requerido.
c) Utilizar cifrado para la protección de información transportada en dispositivos móviles, medios removibles o a través de líneas de comunicación no seguras.
d) El enfoque respecto de la gestión de claves, incluidos los métodos para tratar la protección de las claves criptográficas y la recuperación de la información cifrada en el caso de pérdida, compromiso o daño de las claves.
e) Los roles y las responsabilidades vinculados a la gestión de las claves (incluida su generación), en la que se encontraran vinculados tanto los RAIs responsables como el RTI de la organización.
f) Las normas, políticas y lineamientos que han de adoptarse para la implementación eficaz en toda la organización.
g) El impacto del uso de información cifrada sobre los controles que se basan en la inspección de contenido (por ejemplo: detección de código malicioso).

El CISO será el responsable de la implementación de la presente política.

La toma de decisiones acerca de si una solución criptográfica es la apropiada o no, deberá ser parte de un proceso más amplio de evaluación de riesgos y selección de controles adecuados a la naturaleza y necesidades de la organización.

Al implementar la política, se recomienda considerar las regulaciones y las restricciones nacionales que podrían aplicarse al uso de técnicas criptográficas en diferentes partes del mundo, y las cuestiones relativas al flujo de información cifrada a través de fronteras.

ISO 27.001 A.10.1.1 [1] – ISO 27.002 10.1.1 [14]

IS2.1.16	Nivel C	F

Macroproceso de protección de la información

La organización deberá desarrollar, implementar y mantener una política de gestión de claves criptográficas. Dicha política deberá:

a) Abarcar la gestión de las claves a lo largo de todo su ciclo de vida.
b) Abordar los mecanismos y lineamientos para el uso, protección y vida útil de las claves criptográficas.
c) Establecer los requisitos para la gestión de las claves criptográficas a lo largo de todo su ciclo de vida incluyendo la generación, el almacenamiento, el archivo, la recuperación, la distribución, el retiro y la destrucción de las claves.
d) Asegurarse que la selección de los algoritmos criptográficos, las longitudes de las claves y las prácticas de uso de acuerdo a las buenas prácticas.
e) Asegurar que todas las claves criptográficas se encuentren protegidas contra modificación, pérdida, divulgación y uso no autorizado.
f) Establecer un sistema de gestión de claves criptográficas.

El sistema detallado en f) deberá encontrarse basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

g) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
h) Emitir y obtener certificados de clave pública.

i) Distribuir claves a las entidades previstas, incluyendo cómo se recomienda activar las claves cuando se reciben. j) Almacenar las claves, incluyendo cómo obtienen acceso a las claves los usuarios autorizados. k) Cambiar o actualizar claves, incluyendo reglas sobre cuándo se recomienda cambiar las claves y cómo se lo va a llevar a cabo. l) Tratar con las claves comprometidas. m) Revocar claves, incluyendo cómo se recomienda anularlas o desactivarlas; por ejemplo, cuando las claves han sido comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso también se recomienda archivar las claves). n) Recuperar claves pérdidas o corrompidas. o) Resguardar las claves (actuales e históricas). p) Destruir las claves. q) Registrar y auditar las actividades relativas a la gestión de claves. r) Definir fechas de activación y desactivación de las claves. s) Definir un mecanismo para autenticar las claves públicas. *Los contenidos de los acuerdos o contratos de nivel de servicio con proveedores externos de servicios criptográficos deberán comprender los tópicos de responsabilidad legal, confiabilidad y tiempos de respuesta para la prestación de los servicios.*
ISO 27.001 A.10.1.2 [1] – ISO 27.002 10.1.2 [14]

IS2.1.17	Nivel C	F
Macroproceso de protección de la información		
La organización debe utilizar un protocolo de tiempo de red para mantener a todos los servidores sincronizados con el reloj principal.		
IS1.2.3		
ISO 27.002 12.4.4 [14]		

IS2.1.18	Nivel C	F
Macroproceso de protección de la información		
En función de la protección y aseguramiento de la transferencia de información, la organización deberá: a) Capacitar y formar al personal acerca de tomar las precauciones adecuadas para no revelar información confidencial vinculada a la organización y/o su rol en la organización. b) Utilizar técnicas criptográficas para proteger la confidencialidad, la integridad y la autenticidad de la información. c) Capacitar y formar al personal acerca de no mantener conversaciones confidenciales en lugares públicos o por canales de comunicación inseguros, oficinas y lugares de reunión abiertos. d) Diseñar, implementar y mantener una política de gestión de intercambios de información.		
ISO 27.002 13.2.1 [14]		

IS2.1.19	Nivel C	F
Macroproceso de protección de la información		
Los acuerdos de transferencia de información deberán incorporar: a) Las responsabilidades de la dirección para controlar y notificar el envío, la transmisión y la recepción. b) Los procedimientos para asegurar la trazabilidad, la autenticidad y el no repudio. c) Las normas técnicas mínimas para el empaquetado y la transmisión. d) Los acuerdos de custodia a cargo de terceros. e) Las normas de identificación de los servicios de correo y mensajería. f) Las responsabilidades y las obligaciones en caso de incidentes de SI, tales como pérdida de datos. g) El uso de un sistema de rotulado acordado para la información clasificada con sensibilidad CRÍTICA, ALTA o MEDIA, que asegure que se entienda inmediatamente el significado de los rótulos y que la información se proteja adecuadamente.		

h) Los controles criptográficos que se utilizarán y como serán utilizados.
i) El mantenimiento de la cadena de custodia para la información que está en tránsito.
j) Los niveles aceptables de control de acceso.

Los acuerdos deberán a su vez respetar los lineamientos establecidos en LS1.3.1 y los lineamientos de la política de gestión de intercambios de información.

ISO 27.001 A.13.2.2 [1] - ISO 27.002 13.2.2 [14]

IS2.1.20	Nivel C	F

Macroproceso de protección de la información

La organización deberá desarrollar una Política de Seguridad conjunta con cada parte externa que delinee y documente todos los aspectos, lineamientos y requerimientos fundamentales de la SI en la relación entre estas dos organizaciones para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización. Los lineamientos documentados en la política deberán poseer carácter de cumplimiento obligatorio y se debe a su vez, detallar como se procederá ante un incumplimiento de estos.

Dentro de dicha política, la organización debe identificar y hacer cumplir los controles de SI que traten específicamente el acceso del proveedor a la información de la organización. Se recomienda que estos controles aborden los procesos y procedimientos a ser implementados por la organización, así como aquellos procesos y procedimientos que la organización le requiere al proveedor que implemente, incluyendo:

a) La identificación y documentación de los tipos de proveedores.
b) Un proceso normalizado y un ciclo de vida para la gestión de las relaciones con los proveedores.
c) La definición de los tipos de accesos a la información que se le van a permitir a los distintos tipos de proveedores, y el monitoreo y control de los accesos.
d) Los requisitos mínimos de seguridad para cada tipo de información y de acceso, que sirvan de base para los acuerdos individuales con los proveedores en función de las necesidades de negocio y los requisitos de la organización, y de su perfil de riesgo.

e) Los procesos y los procedimientos para monitorear el cumplimiento de los requisitos establecidos de SI para cada tipo de proveedor y cada tipo de acceso, incluyendo la revisión y la validación de producto por terceras partes.
f) La exactitud y la completitud de los controles para asegurar la integridad de la información o del procesamiento de la información provisto por cualquiera de las partes.
g) Los tipos de obligaciones aplicables a los proveedores para proteger la información de la organización.
h) El manejo de los incidentes y las contingencias asociadas con el acceso del proveedor, incluyendo las responsabilidades tanto de la organización como de los proveedores.
i) Las disposiciones para la resiliencia y si fuera necesario, para la recuperación y la contingencia para garantizar la disponibilidad de la información o del procesamiento de la información provistos por cualquiera de las partes.
j) La capacitación en concientización para el personal de la organización involucrado en las adquisiciones con respecto a las políticas, los procesos y los procedimientos aplicables.
k) La capacitación en concientización para el personal de la organización que interactúa con personal del proveedor con respecto a las reglas apropiadas de intervención y comportamiento en función del tipo de proveedor y el nivel de acceso del proveedor a los sistemas y a la información de la organización.
l) Las condiciones bajo las cuales se van a documentar los requisitos y los controles de SI en un acuerdo firmado por las dos partes.
m) La gestión de las transiciones necesarias de información, de las instalaciones de procesamiento de la información y de cualquier otra cosa que se necesite mover y la garantía de que se mantenga la SI durante todo el período de transición.

Se deben identificar y aplicar controles para administrar el acceso de los proveedores a las instalaciones de procesamiento de la información.

ISO 27.001 A.15.1.1 [1] - ISO 27.002 15.1.1 [14]

IS2.1.21	Nivel C	F

Macroproceso de protección de la información

La organización deberá establecer y acordar todos los requisitos de SI pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o

proporcionar componentes de la infraestructura de TI para la información de la organización. Esto último deberá establecerse y documentarse en acuerdos con sustento legal para obligar a ambas partes a cumplir con todos los requerimientos de seguridad necesarios.

Dichos acuerdos deberán incluir:

a) La descripción de la información a proveer o acceder y los métodos para la provisión o el acceso a la información.
b) La clasificación de la información de acuerdo con el esquema de clasificación de la organización. Si fuera necesario, también una equivalencia entre el esquema de clasificación de la propia organización y el esquema de clasificación del proveedor.
c) Los requisitos legales y reglamentarios, incluyendo la protección de los datos, los derechos de propiedad intelectual y los derechos de autor, y una descripción de la forma en la que se va a garantizar su cumplimiento.
d) La obligación de cada parte en el contrato acerca de la implementación de un conjunto acordado de controles, incluyendo el control de accesos, la revisión del desempeño, el seguimiento, la presentación de informes y la auditoría.
e) Las reglas sobre el uso aceptable de la información, incluyendo el uso inaceptable, si fuera necesario.
f) Las políticas de SI relevantes al contrato específico.
f) Los requisitos y los procedimientos para la gestión de incidentes (especialmente la notificación y la colaboración durante la remediación del incidente).
g) Los requisitos de capacitación y concientización acerca de procedimientos específicos y requisitos de SI, por ejemplo, la respuesta a incidentes o los procedimientos de autorización.
h) Los roles pertinentes al acuerdo, incluyendo una persona de contacto para los asuntos de SI.
i) El derecho a auditar los procesos y los controles del proveedor relacionados con el acuerdo.
j) Los procesos de resolución de defectos y de conflictos.
k) Las obligaciones del proveedor de cumplir con los requisitos de seguridad de la organización.

La organización deberá considerar en el acuerdo los procedimientos para la continuidad del procesamiento en el caso de que el proveedor sea incapaz de proveer sus productos o servicios, a fin de evitar cualquier demora en la obtención de productos o servicios de reemplazo.

ISO 27.001 A.15.1.2 [1] - ISO 27.002 15.1.2 [14]

IS2.1.22	Nivel C	F

Macroproceso de protección de la información

Los acuerdos de la organización con los proveedores deben incluir requisitos para tratar los riesgos a la SI asociados a la cadena de suministro de servicios y productos de las tecnologías de la información de las comunicaciones.

Los acuerdos deben incluir:

a) La definición de los requisitos de SI a aplicar en la adquisición de productos o servicios de las tecnologías de la información y las comunicaciones adicionalmente a los requisitos de SI en las relaciones con los proveedores.
b) Para los servicios de tecnologías de la información y las comunicaciones, el requisito de que los proveedores propaguen los requisitos de seguridad de la organización a lo largo de toda la cadena de suministros si los proveedores subcontratan partes del servicio de tecnologías de la información y las comunicaciones a otros proveedores.
c) Para los productos de tecnologías de la información y las comunicaciones, el requisito de que los proveedores propaguen las prácticas apropiadas de seguridad a lo largo de toda la cadena de suministros si estos productos incluyen componentes comprados a otros proveedores.
d) La implementación de un proceso de monitoreo y de métodos aceptables para validar que los productos y servicios de las tecnologías de la información y las comunicaciones provistos, cumplen con los requisitos de seguridad declarados.
e) La obtención del aseguramiento de que los componentes críticos y su origen sean trazables a lo largo de toda la cadena de suministro.
f) La obtención del aseguramiento de que los productos de las tecnologías de la información y las comunicaciones provistos funcionan de la manera esperada sin características inesperadas o indeseadas.
g) La definición de reglas para compartir la información en lo referente a la cadena de suministro y de cualquier problema o compromiso potencial entre la organización y los proveedores.

La organización debe trabajar con sus proveedores para comprender la cadena de suministro de las tecnologías de la información y las comunicaciones y

cualquier tema que pueda tener un impacto importante sobre los productos y servicios provistos.
ISO 27.001 A.15.1.3 [1] - ISO 27.002 15.1.3 [14]

IS2.1.23	Nivel C	F
Macroproceso de protección de la información		
La organización deberá seguir, auditar y revisar periódicamente la entrega de los servicios prestados por proveedores, con el objetivo de garantizar que se cumplan los términos y las condiciones de SI (incluidos en los acuerdos) y que los incidentes y los inconvenientes de SI se gestionen de forma apropiado y según los mecanismos acordados. Para lo cual, se deberá diseñar, implementar y mantener un proceso de gestión de servicios entre la organización y el proveedor. Dicho proceso deberá: a) Seguir y controlar los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos. b) Revisar los informes del servicio producidos por el proveedor y concertar reuniones periódicas según lo requieran los acuerdos. c) Realizar auditorías a los proveedores, junto a la revisión de los informes de los auditores independientes, si estuvieran disponibles, y seguir los problemas identificados. d) Verificar el cumplimiento de los lineamientos establecidos en LS1.3.1.		
ISO 27.001 A.15.2.1 [1] - ISO 27.002 15.2.1 [14]		

IS2.1.24	Nivel C	F
Macroproceso de protección de la información		
Los cambios en la prestación de los servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de SI existentes, deben gestionarse teniendo en cuenta la criticidad de		

la información, sistemas y procesos de negocio involucrados y la reevaluación de los riesgos.

Algunos de los cambios que deben considerarse son los siguientes:

a) Los cambios en los servicios de los proveedores para implementar nuevas tecnologías, modificaciones al servicio, nuevas herramientas o entornos o la subcontratación de otro proveedor.
b) Los cambios en los acuerdos con los proveedores.
c) Los cambios realizados por la organización para implementar mejoras a los servicios, desarrollos, modificaciones o actualizaciones y nuevos controles de seguridad o versiones mejoradas de estos.

ISO 27.001 A.15.2.2 [1] - ISO 27.002 15.2.2 [14]

IS2.1.25	Nivel B	F

Macroproceso de protección de la información

Para el cifrado de toda información clasificada con sensibilidad CRITICA o ALTA, se deberán cumplir los siguientes lineamientos:

a) Se deberá realizar múltiples niveles de cifrados (utilizando al menos dos algoritmos de cifrado diferentes), cada uno con una clave de descifrado distinta. En el caso de claves o atajos que el usuario debe ingresar para realizar el descifrado no deberán ser menores a los 30 caracteres y deberán poseer al menos 5 caracteres en minúscula diferentes, 5 caracteres en mayúscula diferentes, 5 caracteres numéricos diferentes y 5 caracteres especiales diferentes.
b) El tamaño de la clave deberá ser considerablemente mayor al mínimo recomendado por normas, estándares y la comunidad de SI.
c) Se deberán utilizar únicamente algoritmos de cifrado cuyo mecanismo sea totalmente público y hayan sido probados por un tiempo prudente por la comunidad de SI.
d) No se podrán almacenar digitalmente las claves o atajos que el usuario debe ingresar para realizar el descifrado. De guardarlas físicamente, deberán ser almacenadas en forma segura dentro de una caja fuerte asegurada que se encuentre dentro de un área restringida de la organización. Las claves o atajos no podrán abandonar el área restringida.

El apartado c) será de cumplimiento obligatorio para todo tipo de información de la organización.

IS2.1.26	Nivel B	F
Macroproceso de protección de la información		
Los acuerdos de transferencia de información deberán: a) Incorporar procedimientos destinados a proteger la información y los medios físicos en tránsito. b) Reflejar la sensibilidad de la información de negocio involucrada. c) Tener forma de contratos formales y haber sido suscriptos por representantes legales de cada organización. Deben tener valor legal.		
ISO 27.001 A.13.2.2 [14]		

IS2.1.27	Nivel B	F
Macroproceso de protección de la información		
Los acuerdos con proveedores establecidos en IS2.1.21 deberán, a su vez, incluir: a) Una lista explícita de personal del proveedor autorizado, o los procedimientos o las condiciones para la autorización y la desautorización del personal del proveedor, para acceder o recibir información de la organización. b) Las reglamentaciones pertinentes a la subcontratación, incluyendo los controles que se necesita implementar. c) Los requisitos, si los hubiera, para la investigación de antecedentes del personal del proveedor, incluyendo las responsabilidades por la realización de la investigación de antecedentes y los procedimientos para la notificación en caso de que la investigación no se haya completado o si los resultados fueran motivo de dudas o preocupaciones.		

d) La obligación del proveedor a presentar periódicamente un informe independiente sobre la eficacia de los controles y el acuerdo de corregir puntualmente todos los problemas mencionados en el informe.
IS2.1.21
ISO 27.001 A.15.1.2 [1] - ISO 27.002 15.1.2 [14]

IS2.1.28	Nivel B	F
Macroproceso de protección de la información		
Los acuerdos con proveedores establecidos en IS2.1.22 deben incluir: a) La implementación de un proceso para identificar los componentes de los productos o servicios que son críticos para mantener la funcionalidad y que, por lo tanto, requieren de mayor atención y escrutinio cuando se los implementa fuera de la organización, especialmente si el proveedor directo subcontrata aspectos de los componentes de los productos o servicios a otros proveedores. b) La implementación de procesos específicos para gestionar el ciclo de vida de los componentes de las tecnologías de la información y las comunicaciones, y su disponibilidad y los riesgos de seguridad asociados. Esto incluye la gestión de los riesgos de componentes que ya no estén disponibles debido a que los proveedores ya no se encuentran activos o que ya no proporcionan esos componentes debido a los avances tecnológicos. Las organizaciones deben trabajar con sus proveedores para comprender la cadena de suministro de las tecnologías de la información y las comunicaciones y cualquier tema que pueda tener un impacto importante sobre los productos y servicios provistos.		
ISO 27.001 A.15.1.3 [1] - ISO 27.002 15.1.3 [14]		

IS2.1.29	Nivel C	F
Macroproceso de protección de la información		
El proceso de gestión de servicios entre la organización y sus proveedores deberá:		

a) Proveer información sobre los incidentes de SI y revisar esta información según lo requieran los acuerdos y todas las directrices o los procedimientos de apoyo.
e) Revisar las pistas para la auditoría del proveedor y sus registros de eventos de SI, los problemas operativos, las fallas, los hallazgos de defectos y las interrupciones relacionadas con el servicio prestado.
f) Resolver y gestionar todos los problemas identificados.
g) Revisar los aspectos de SI en las relaciones del proveedor con sus propios proveedores.
h) Garantizar que el proveedor mantenga una capacidad de servicio suficiente, junto con los planes viables diseñados para garantizar que se mantengan los niveles acordados de continuidad luego de un desastre o de una falla mayor del servicio.

Se debe asignar la responsabilidad por la gestión de la relación con los proveedores a una persona designada o a un equipo de gestión de servicios.

La organización deberá disponer de las capacidades y los recursos técnicos suficientes para el seguimiento de los requisitos de los acuerdos, en particular que se cumplan los requisitos de SI. Se recomienda realizar las acciones apropiadas cuando se observen deficiencias en la prestación de servicios.

La organización debe mantener la visibilidad de las actividades de seguridad tales como la gestión de cambios, la identificación de vulnerabilidades, el reporte y la respuesta a los incidentes de SI a través de un proceso definido.

ISO 27.001 A.15.2.1 [1] - ISO 27.002 15.2.1 [14]

IS2.1.30	Nivel B	F

Macroproceso de protección de la información

La organización deberá diseñar, implementar y mantener las siguientes políticas:

a) Política de Privacidad & Protección de los datos personales identificables ("*personal identifiable data*"), aquellos datos de partes interesadas que faciliten la identificación de una persona física o jurídica. Dicha política deberá establecer los lineamientos, controles y procesos a implementar y mantener por la organización para lograr la confidencialidad, integridad y disponibilidad de los datos personales identificables en todo momento.

b) Política de gestión de la relación con proveedores. Dicha política establecerá los lineamientos de SI para la gestión con los proveedores. Se deberá a su vez establecer una política de gestión de la relación con partes interesadas que gobernará a la presente política.
IS2.1.21
ISO 27.001 A.15.1.2 [1] - ISO 27.002 15.1.2 [14]

IS2 PROTECCIÓN Y DEFENSA DE LA SEGURIDAD

IS2.2 Gestión de incidentes de SI

Objetivo Establecer los fundamentos de la gestión de los incidentes de Seguridad de la Información de la organización, uno de los aspectos primordiales de la Seguridad de la Información ya que, aprendiendo de ellos podremos efectivamente mejorar el nivel general de seguridad de la organización y por ende su estadio de madurez de seguridad.

IS2.2.1	Nivel E	F
Macroproceso de defensa de la información		
Se deben establecer las responsabilidades y los procesos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de SI. Se deberá asignar las responsabilidades dentro de la dirección ejecutiva de: a) El tratamiento del incidente de SI. b) La investigación de las causas del incidente de SI. c) El diseño e implementación de iniciativas destinadas a solucionar el origen del incidente. La organización deberá establecer un proceso formal disciplinario para ocuparse de los empleados (incluyendo contratistas y de terceras partes) que cometan violaciones de SI.		

ISO 27.001 A.16.1.1 [1] – ISO 27.002 16.1.1 [14]

IS2.2.2	Nivel E	F
Macroproceso de defensa de la información		
Los eventos de SI se deben informar a través de canales de gestión apropiados, tan pronto como sea posible. La organización debe requerir que los empleados, contratistas y usuarios de terceras partes que utilicen los sistemas y servicios de información de la organización informen cualquier vulnerabilidad de SI observada o sospechada en sistemas, servicios, dispositivos, recursos y locaciones. Todos los empleados, contratistas y usuarios de terceras partes deberán ser conscientes: a) Su responsabilidad de reportar cualquier evento de SI tan pronto como sea posible. Para lo cual, la organización establecerá un proceso sencillo y accesible de reporte de eventos de seguridad. b) Del proceso de reporte de incidentes de SI y del punto de contacto al cual se deben reportar los eventos de seguridad.		
ISO 27.001 A.16.1.2 y A.16.1.3 [1] – ISO 27.002 16.1.2 y 16.1.3 [14]		

IS2.2.3	Nivel D	F
Macroproceso de defensa de la información		
La organización deberá documentar que acciones y acontecimientos serán considerados como eventos de seguridad en adición a lo siguiente: a) Control de seguridad ineficaz. b) Violación de la integridad, la confidencialidad o la disponibilidad esperada. c) Errores humanos. d) Los no cumplimientos con las políticas o directrices.		

e) Las violaciones de los mecanismos de seguridad física. f) Los cambios no controlados en el sistema. g) El mal funcionamiento o comportamiento anómalo del software o del hardware. h) Las violaciones de acceso.
ISO 27.002 16.1.2 [14]

IS2.2.4	Nivel D	F
Macroproceso de defensa de la información		
La organización deberá advertir a los usuarios (propios, contratados y de terceras partes) que no intenten probar las debilidades de seguridad sospechadas, con excepción de aquellos autorizados a investigar vulnerabilidades o realizar pruebas de penetración.		
ISO 27.002 16.1.3 [14]		

IS2.2.5	Nivel D	F
Macroproceso de defensa de la información		
Las responsabilidades y procesos de gestión de incidentes de SI (detallados en IS2.2.1) deberán contemplar: a) Mantener los contactos apropiados con las autoridades, grupos de interés o foros externos relacionados a la gestión de problemas y/o incidentes de SI. b) La implementación de un punto de contacto para la detección y el reporte de incidentes de SI. c) El diseño, implementación y mantenimiento del proceso a ejecutar en caso de ocurrencia de un incidente de SI (que contemple actividades como tomar nota de los detalles del incidente o reportar inmediatamente el incidente al punto de contacto.		
IS2.2.1		
ISO 27.002 16.1.1 [14]		

IS2.2.6	Nivel C	F
Macroproceso de defensa de la información		
La organización deberá diseñar, establecer y mantener los siguientes procesos vinculados a la gestión de incidentes de SI: a) Planificación y preparación de la respuesta a incidentes de SI. b) El seguimiento, la detección, el análisis y la notificación de los eventos y los incidentes de SI. c) El registro de las actividades de gestión de incidentes. d) La manipulación de la evidencia forense. e) La evaluación y la toma de decisiones sobre los eventos de SI y la evaluación de las debilidades de SI. f) La respuesta, incluyendo aquellos que se escalaran jerárquicamente en la organización, la recuperación controlada ante un incidente y la comunicación a actores internos o externos. g) Reporte de incidentes de SI.		
ISO 27.002 16.1.1 [14]		

IS2.2.7	Nivel C	F
Macroproceso de defensa de la información		
La organización deberá asegurarse que el personal responsable de gestionar todos los temas relacionados a la gestión de incidentes de SI se encuentre adecuadamente capacitado y sea competente para desarrollar sus tareas. A su vez, deberán comprender las prioridades de la organización para el manejo de los incidentes de SI, en función de los objetivos de gestión de incidentes de SI.		
ISO 27.002 16.1.1 [14]		

IS2.2.8	Nivel C	F
Macroproceso de defensa de la información		
La organización deberá desarrollar, implementar y mantener una la política de gestión de incidentes de SI. Los objetivos de gestión de incidentes de SI deberán establecerse en acuerdo con la dirección ejecutiva de la organización. Dichos objetivos deberán documentarse dentro de la política de gestión de incidentes de SI de la organización.		
ISO 27.002 16.1.1 [14]		

IS2.2.9	Nivel C	F
Macroproceso de defensa de la información		
Se debe evaluar los eventos de SI y decidir si se los debe calificar como incidentes de SI. El punto de contacto establecido por la organización deberá evaluar cada evento de seguridad utilizando una escala de clasificación acordada para eventos e incidentes para así decidir si corresponde clasificar el evento como un incidente de SI. Se debe documentar tanto la evaluación del evento como la decisión o no de clasificarlo como un incidente de SI. *Si la organización posee un equipo de respuesta a incidentes de SI, se recomienda que evaluación del evento y posterior decisión sea delegado al mismo.*		
ISO 27.001 A.16.1.4 [1] – ISO 27.002 16.1.4 [14]		

IS2.2.10	Nivel C	F
Macroproceso de defensa de la información		
La organización debe responder a los incidentes de SI de acuerdo con los procedimientos de respuesta documentados. La respuesta a los incidentes de SI estará a cargo del punto de contacto nominado (a menos que la organización posea un equipo de respuesta a incidentes de seguridad tal como se menciona en IS2.2.9) y otras personas pertinentes de la organización o terceras partes. La respuesta a los incidentes de SI deberá como mínimo abarcar: a) La recolección de evidencia lo antes posible luego de que ocurra el incidente. b) La realización de un análisis forense de SI. c) El escalamiento, de corresponder. d) El registro y documentación de todas las actividades de respuesta. e) La comunicación de la existencia del incidente y sus correspondientes detalles a todas las partes interesadas (internas y externas) con necesidad de saber. f) El tratamiento de las debilidades de SI que se conoce causaron o contribuyeron al incidente. g) El cierre y el registro del incidente, una vez que éste fue tratado satisfactoriamente. Una vez solucionado preliminarmente el incidente (una vez asegurado el nivel de seguridad normal y luego de haber iniciado la recuperación necesaria), se deberá realizar un análisis de causa-raíz para identificar la fuente de la causa del incidente pasa así solucionarlo en el largo plazo y evitar su reiteración en el tiempo.		
ISO 27.001 A.16.1.5 [1] – ISO 27.002 16.1.5 [14]		

IS2.2.11	Nivel C	F
Macroproceso de defensa de la información		
Se debe utilizar el conocimiento obtenido del análisis y resolución de los incidentes de SI para reducir la probabilidad o el impacto de futuros incidentes.		

La evaluación de los incidentes dará inicio al diseño de modificaciones y mejoras al Sistema de Mejora Continua en SI de la organización.
ISO 27.001 A.16.1.6 [1] – ISO 27.002 16.1.6 [14]

IS2.2.12	Nivel C	F
Macroproceso de defensa de la información		
La organización debe definir y aplicar procesos formales para la identificación, recolección, adquisición y preservación de la información que pueda utilizarse como evidencia. Los procesos deberán diseñarse tomando en cuenta que la evidencia podría llegar a ser utilizada en una acción legal/judicial o disciplinaria. Los procesos deberán tener en cuenta: a) La cadena de custodia. b) la integridad física de la evidencia y del personal. c) La documentación a relevar y a generar. d) Los roles y las responsabilidades del personal involucrado. e) La competencia del personal que ejecuta el proceso. f) La consideración de los requisitos de diferentes jurisdicciones para maximizar las posibilidades de admisión en todas las jurisdicciones pertinentes. g) Asegurarse que la organización tenga el derecho de recolectar la información requerida como evidencia forense. *Se recomienda que la organización procure obtener personal o herramientas certificados o calificados externos, de manera de robustecer el valor de la evidencia preservada.*		
ISO 27.001 A.16.1.7 [1] – ISO 27.002 16.1.7 [14]		

IS2.2.13	Nivel B	F
Macroproceso de defensa de la información		
La organización deberá establecer los procesos adecuados de retroalimentación para garantizar que a aquellas personas que reporten eventos de SI se les notifiquen los resultados una vez que el problema haya sido tratado y cerrado.		
ISO 27.002 16.1.1 [14]		

IS2.2.14	Nivel B	F
Macroproceso de defensa de la información		
Se deben establecer mecanismos que permitan cuantificar y monitorear los tipos, los volúmenes y los costos de los incidentes de SI. La información obtenida de la evaluación de los incidentes de SI debe ser utilizada para identificar aquellos incidentes recurrentes o de alto impacto.		
ISO 27.002 16.1.6 [14]		

IS2.2.13	Nivel B	F
Macroproceso de defensa de la información		
La organización deberá obtener personal o herramientas certificados o calificados externos, de manera de robustecer el valor de la evidencia preservada.		
ISO 27.002 16.1.1 [14]		

[Página dejada en blanco intencionalmente]

GESTIÓN DE LA TECNOLOGÍA

El presente subsistema de seguridad del MRU se enfoca fundamentalmente en el establecimiento de los lineamientos y controles necesarios para el uso correcto y seguro de la Tecnología de la Información.

Se enfoca principalmente en la seguridad tanto del software como del hardware tanto propio de la organización como aquel utilizado por la misma o por sus usuarios. A su vez. Establecerá los lineamientos de madurez vinculados a los conocidos niveles TIER para el centro de cómputos propio o tercerizado de la organización.

GT1 Seguridad de los sistemas y la Tecnología

GT1.1 Tecnología de Seguridad de la Información

GT1.2 Gestión de sistemas de Información

GT2 Gestión de la Tecnologías de la Información

GT2.1 Lineamientos de gestión y eficiencia operativa

GT1 SEGURIDAD DE LOS SISTEMAS Y LA TECNOLOGÍA

GT1.1 Tecnología de la SI

Objetivo Gestionar los lineamientos y procesos de Seguridad de la Información enfocados al uso correcto y seguro de la tecnología para las actividades del negocio. Aquí se tratarán los lineamientos de seguridad para el teletrabajo, dispositivos móviles y la conocida metodología BYOD.

GT1.1.1	Nivel E	F
Proceso de gestión de dispositivos móviles		
La organización deberá definir: a) Que es considerado como dispositivo móvil, abarcando al menos a los celulares, las tabletas y las computadoras portátiles. b) Si permite o no el ingreso a sus instalaciones de dispositivos móviles que no sean ni propiedad de la organización ni se encuentran bajo su custodia. c) Si permite o no el ingreso a sus áreas restringidas de dispositivos móviles que no sean ni propiedad de la organización ni se encuentran bajo su custodia. El resultado del apartado a) deberá encontrarse adecuadamente documentado.		

GT1.1.2	Nivel D	F
Proceso de gestión de dispositivos móviles		
En cuanto a dispositivos móviles, la organización deberá: a) Diseñar, establecer y mantener una política de gestión dispositivos móviles. b) Definir la aplicación o no de una política amigable ("*BYOD*[48]") con los dispositivos propios de los empleados, contratistas o terceras partes, en función de GT1.1.1.b y GT1.1.1.c. La definición del apartado b) deberá encontrarse adecuadamente documentada dentro de la política de gestión dispositivos móviles. La política de gestión dispositivos móviles deberá: c) Establecer los lineamientos de uso de dispositivos móviles para las actividades del negocio. d) Establecer las medidas de SI estratégicas que se implementarán para regular su uso. e) Tener en cuenta los riesgos que implica el uso de dispositivos móviles en entornos no protegidos.		
GT1.1.1.b – GT1.1.1.c		
ISO 27.001 A.6.2.1 [1] - ISO 27.002 6.2.1 [14]		

GT1.1.3	Nivel D	F
Macroproceso de gestión de redes		
La organización deberá diseñar, establecer y mantener una política de uso de las redes y los servicios de red. La misma establecerá: a) Los lineamientos de seguridad, control de acceso y segregación de redes y servicios de red que la organización considere necesarios. b) La obligación de proveer a los usuarios (propios, contratistas o de terceras partes) únicamente el acceso a la red y a los servicios a los cuales han sido específicamente autorizados a utilizar.		

[48] Por sus siglas en inglés: Trae tu propio dispositivo ("*Bring your own device*").

ISO 27.001 A.9.1.2 [1] - ISO 27.002 9.1.2 [14]

GT1.1.4	Nivel D	F
Macroproceso de gestión de redes		
Se deben implementar controles de detección, prevención y recuperación para la protección contra software malicioso, combinados con la concientización apropiada de los usuarios. La protección debe basarse en software para la detección de código malicioso y reparación, en la concientización sobre SI y en los controles apropiados para la gestión del cambio y acceso a los sistemas. *Se recomienda tener el cuidado de proteger contra la introducción de código malicioso durante los procedimientos de mantenimiento y de emergencia, los cuales pueden evadir los controles normales de protección contra código malicioso.*		
ISO 27.001 A.12.2.1 [1] - ISO 27.002 12.2.1 [14]		

GT1.1.5	Nivel D	F
Macroproceso de gestión de redes		
La organización deberá proteger apropiadamente la información involucrada en la mensajería electrónica, en función de los siguientes lineamientos: a) Protección de los mensajes contra el acceso no autorizado, la modificación o la denegación de servicio de manera proporcional al esquema de clasificación adoptado por la organización. b) Aseguramiento del correcto direccionamiento y transporte del mensaje. c) Confiabilidad y la disponibilidad del servicio. d) Consideraciones legales. e) Obtención de aprobación previa al uso de servicios públicos externos tales como mensajería instantánea, redes sociales o archivos compartidos.		

f) Niveles altos del control de autenticación para los accesos desde redes accesibles al público.
ISO 27.001 A.13.2.3 [1] - ISO 27.002 13.2.3 [14]

GT1.1.6	Nivel D	F
Macroproceso de gestión de redes		
La organización deberá gestionar y controlar las redes para proteger la información en sistemas y aplicaciones, en función de los siguientes lineamientos: a) Establecer las responsabilidades y los procesos para la gestión del equipamiento de red. b) Que la responsabilidad operativa por las redes se encuentre separada de las operaciones del restante equipamiento informático, cuando corresponda. c) Verificar que se establezcan controles especiales para salvaguardar la confidencialidad y la integridad de los datos que se transmiten por redes públicas o por redes inalámbricas y para proteger a los sistemas y a las aplicaciones conectados. d) Asegurarse que se registre y monitoree apropiadamente para permitir la detección de las acciones que puedan afectar o sean relevantes a la SI. e) Asegurarse que las actividades de gestión se encuentren estrechamente coordinadas, tanto para optimizar el servicio a la organización como para garantizar que los controles se aplican consistentemente a través de toda la infraestructura de procesamiento de la información. f) Autenticar los sistemas en la red. g) Restrinja la conexión de sistemas a la red.		
ISO 27.001 A.13.1.1 [1] - ISO 27.002 13.1.1 [14]		

GT1.1.7	Nivel D	F
Proceso de gestión de software		
La organización deberá establecer e implementar reglas que gobiernen la instalación de software por parte de los usuarios. Para lo cual deberá definir y hacer cumplir una política estricta acerca de los tipos de software que los usuarios pueden instalar. La misma se encontrará basada en los siguientes lineamientos: a) Aplicación del principio del mínimo privilegio. b) Identificación de los tipos de instalaciones de software que están permitidos. c) Identificación de los tipos de instalaciones que están prohibidos. d) Otorgar privilegios en función de los roles de los usuarios involucrados.		
ISO 27.001 A.12.6.2 [1] - ISO 27.002 12.6.2 [14]		

GT1.1.8	Nivel C	F
Proceso de gestión de dispositivos móviles		
La política de gestión dispositivos móviles deberá establecer lineamientos sobre: a) El registro de los dispositivos móviles (incluyendo aquellos que son de propiedad de empleados o terceras partes). b) Los requisitos para la protección física de los dispositivos móviles (especialmente contra robo de estos). c) La restricción de instalaciones de software. d) Los requisitos para las versiones de software del dispositivo móvil y para la aplicación de parches. e) Los controles de acceso a los activos de información, sistemas, herramientas y servicios de la organización. f) Las técnicas criptográficas a utilizar para proteger la información en tránsito como la que será almacenada dentro del dispositivo móvil. g) La protección contra software malicioso. h) Copias de respaldo de la información manipulada desde los dispositivos móviles y la información almacenada en estos.		

i) El uso de los servicios y aplicaciones web para desarrollar actividades del negocio.
j) El establecimiento de barreras de acceso no autorizado y protección de los dispositivos móviles (tales como contraseñas, bloqueo de sesión, entre otras).
k) Formación y capacitación de todo el personal, contratistas y terceras partes para la utilización segura de dispositivos móviles y cumplimiento de los lineamientos de la política de gestión dispositivos móviles.
l) Legislación en materia de privacidad (específicamente para el establecimiento de controles de monitoreo de la actividad, protección contra software malicioso y borrado remoto en caso de robo, perdida, extravió o desvinculación del usuario).
m) La inactivación, borrado y bloqueo remoto.

La organización solo deberá proporcionar acceso a la información de negocio luego de que el usuario (propio, contratista o de tercera parte) haya firmado un acuerdo de usuario final reconociendo sus obligaciones (protección física. Actualización de software, bloqueo del dispositivo al no utilizarlo, entre otros), renunciando a la propiedad de los datos de negocio, permitiendo el borrado remoto de los datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no se tenga autorización para utilizar el servicio. Esta política necesita tener en cuenta la legislación de privacidad.

ISO 27.002 6.2.1 [14]

GT1.1.9	Nivel C	F

Macroproceso de gestión de redes

La política de uso de las redes y los servicios de red de la organización deberá establecer lineamientos de seguridad que abarquen los siguientes temas:

a) Las redes y los servicios de red a los cuales se permite el acceso.
b) Los procedimientos de autorización para determinar quién puede tener acceso a qué redes y servicios de red.
c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.
d) Los medios utilizados para acceder a las redes y los servicios de red (por ejemplo, el uso de una red privada virtual o una red inalámbrica).

e) Los requisitos de autenticación del usuario para acceder a los distintos servicios de red.
f) El monitoreo del uso de los servicios de red.

La política deberá integrarse y ser coherente con la política de gestión de accesos de la organización.

ISO 27.002 9.1.2 [14]

GT1.1.10	Nivel C	F

Subproceso de gestión de la capacidad

La organización deberá realizar un seguimiento y ajustar el uso de recursos en función de las proyecciones de futuros requisitos de capacidad para asegurar el desempeño requerido del sistema, en función de los siguientes lineamientos:

a) Los requisitos de capacidad deben identificarse en función de la criticidad para el negocio del sistema involucrado.
b) Se debe optimizar y monitorear el sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficacia de los sistemas.
c) Se deben establecer controles para la detección oportuna de problemas.
d) Las proyecciones de futuros requisitos de capacidad deberán tener en cuenta los nuevos requisitos del negocio y de los sistemas, y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.

Se necesita prestar particular atención a cualquier recurso que demande mucho tiempo de adquisición o alto costo, por lo que se recomienda que los gerentes realicen un seguimiento de la utilización de los recursos clave del sistema. Los administradores deberán identificar tendencias en el uso, particularmente en relación con las aplicaciones de negocio o con las herramientas de gestión de los sistemas de información.

Los responsables funcionales utilizarán esta información para identificar y evitar potenciales cuellos de botella y la dependencia del personal clave que podría significar una amenaza a la seguridad o a los servicios del sistema, y para planificar las acciones apropiadas.

La capacidad trata a su vez de recursos humanos, oficinas, instalaciones y demás tipos de recursos.
ISO 27.001 A.12.1.3 [1] - ISO 27.002 12.1.3 [14]

GT1.1.11	Nivel C	F
Proceso de gestión de software		
La organización deberá establecer una política formal que prohíba el uso de software no autorizado. A su vez, deberá: a) Implementar controles que prevengan o detecten el uso de software no autorizado. b) Aislar los entornos en los cuales pueda ocurrir un impacto catastrófico. c) Implementar controles que prevengan o detecten el uso de sitios web conocidos o sospechados de maliciosos. d) Establecer una política formal para proteger contra los riesgos asociados con la obtención de archivos y software, ya sea desde o a través de redes externas, o por cualquier otro medio, indicando qué medidas de protección se recomienda tomar. e) Reducir las vulnerabilidades que el código puede explotar. f) Realizar revisiones periódicas del contenido de software y datos de los sistemas que sustentan los procesos críticos del negocio e investigar formalmente la presencia de cualquier archivo no aprobado o de cualquier modificación no autorizada. g) La instalación y la actualización periódica del software para la detección del código malicioso y para la reparación para verificar computadoras y medios como control preventivo o periódico. h) Definir los procedimientos y las responsabilidades para ocuparse de la protección contra código malicioso en los sistemas, capacitar sobre su uso, informar y recuperarse de los ataques de código malicioso; i) Diseñar y establecer planes de continuidad del negocio para la recuperación ante ataques de código malicioso, incluyendo todos los acuerdos y mecanismos necesarios para el resguardo y la recuperación de los datos y el software.		

j) Implementar procedimientos para recolectar información periódicamente, tales como la suscripción a listas de correo o la verificación de los sitios de Internet que brindan información acerca de nuevo código malicioso;
k) Implementar procedimientos para verificar la información relacionada con el código malicioso y asegurar que los boletines de alerta sean exactos e informativos.

ISO 27.001 A.12.2.1 [1] - ISO 27.002 12.2.1 [14]

GT1.1.13	Nivel C	F

Macroproceso de gestión de redes

La organización deberá identificar e incluir en cualquier acuerdo de servicios de red, los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sean servicios provistos por la organización o terceras partes.

Por lo que, debe:

a) Determinar y monitorear periódicamente la capacidad del prestador del servicio de red para gestionar los servicios acordados en un modo seguro, y acordar el derecho de auditarlo.
b) Identificar los acuerdos de seguridad necesarios para servicios particulares, tales como las características de seguridad, los niveles de servicio y los requisitos de gestión. Se recomienda que la organización se asegure de que los proveedores de servicios de redes implementen estas medidas.

Los servicios de red incluyen la provisión de las conexiones, servicios de red privados y redes de valor agregado, y soluciones de seguridad en redes tales como "firewalls" y sistemas de detección de intrusos. Estos servicios pueden variar desde un simple ancho de banda no gestionado hasta ofertas complejas con valor agregado.

ISO 27.001 A.13.1.2 [1] - ISO 27.002 13.1.2 [14]

GT1.1.14	Nivel C	F
Macroproceso de gestión de redes		
La organización deberá segregar en más de una red a los grupos de servicios de información, los usuarios y los sistemas de información. Para lo cual la organización debe: a) Definir correctamente el perímetro de cada dominio en base a la política de gestión de accesos. b) Controlar el acceso entre dominios de red utilizando un gateway. c) Considerar el tratamiento de todos los accesos inalámbricos como conexiones externas y la segregación de estos accesos inalámbricos respecto de las redes internas hasta que hayan pasado a través de un gateway de acuerdo con la política de controles de red.		
ISO 27.001 A.13.1.3 [1] - ISO 27.002 13.1.3 [14]		

GT1.1.15	Nivel C	F
Macroproceso de gestión de redes		
La organización deberá obtener información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan, evaluar la exposición de la organización a tales vulnerabilidades, y tomar las medidas apropiadas para tratar los riesgos asociados. Por lo que debe tomar una acción oportuna y apropiada en respuesta a la identificación de las vulnerabilidades técnicas potenciales en función de los siguientes lineamientos: a) La organización debe definir y establecer los roles y responsabilidades asociados con la gestión de las vulnerabilidades técnicas, incluyendo el monitoreo de la vulnerabilidad, la evaluación de los riesgos de la vulnerabilidad, los parches, el rastreo de activos y cualquier responsabilidad de coordinación requerida. b) Que se identifiquen, para el software y otras tecnologías, los recursos de información que se van a usar para identificar las vulnerabilidades técnicas pertinentes y concientizar sobre ellas. c) Que se defina un plazo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente pertinentes.		

d) Que la organización identifique los riesgos asociados y las acciones a llevar a cabo, una vez que se ha identificado una vulnerabilidad técnica potencial.
e) Que la acción tomada se lleve a cabo de acuerdo con los controles relacionados con la gestión del cambio o siguiendo los procedimientos de respuesta a incidentes de SI, dependiendo de la urgencia con la que se deba tratar la vulnerabilidad técnica.
f) Si hay un parche disponible de una fuente legítima, que se evalúen los riesgos asociados a la instalación del parche.
g) Que se prueben y evalúen los parches antes de instalarlos para asegurar que sean eficaces y que no posean efectos secundarios que no se puedan tolerar.
h) Que se mantenga un registro para la auditoría de todos los procedimientos realizados.
i) Que periódicamente se realice monitoreo y evaluación del proceso de gestión de las vulnerabilidades técnicas para garantizar su eficacia y eficiencia.
j) Que se traten primero los sistemas de alto riesgo.
k) Que el proceso de gestión de vulnerabilidades técnicas se alinee con las actividades de gestión de incidentes para comunicarle los datos sobre las vulnerabilidades al responsable de respuesta a incidentes y proporcionar procedimientos técnicos a llevar a cabo en caso de ocurrir un incidente.
l) Definir un procedimiento para tratar una situación en la cual se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada.

ISO 27.001 A.12.6.1 [1] - ISO 27.002 12.6.1 [14]

GT1.1.16	Nivel B	F

Proceso de gestión de medios removibles

La organización deberá establecer un procedimiento específico que tenga en cuenta los requisitos legales, de seguros y de seguridad para casos de robo, perdida o extravió de los dispositivos móviles.

A su vez, se deberá:

a) Separar el uso privado y de negocio de los dispositivos, incluyendo el uso de software para soportar dicha separación y proteger los datos de negocio en un dispositivo privado.
b) Utilizar un MDM para la gestión de todos los dispositivos móviles.

c) Utilizar el concepto de “ping de vida”. d) Establecer una tienda de aplicaciones propias de la organización y limitar el uso de software a aplicaciones de esa tienda (en todo el dispositivo o en la sección destinada al negocio según el apartado a)). No se deberán dejar desatendidos los dispositivos que transporten información clasificada con sensibilidad ALTA o CRÍTICA. Estos dispositivos deberán: e) Almacenarse bajo llave, en momentos de no uso del mismo. f) Poseer bloqueos especiales (tantos criptográficos como de acceso).
ISO 27.002 6.2.1 [14]

GT1 SEGURIDAD DE LOS SISTEMAS Y LA TECNOLOGÍA

GT1.2 Gestión de Sistemas de Información

Objetivo Establecer los fundamentos y lineamientos de Seguridad de la Información para el desarrollo, diseño, adquisición, pasaje a producción, mantenimiento y gestión de los sistemas de información vinculados a la organización.

GT1.2.1	Nivel D	F
Subproceso de gestión de requisitos		
La organización deberá incluir los requisitos relacionados con la SI dentro de los requisitos para los nuevos sistemas de información o las mejoras de los existentes. Los requisitos de SI se identificaran utilizando métodos diversos tales como derivar los requisitos de cumplimiento a partir de las políticas y reglamentaciones, el modelado de amenazas, la revisión de los incidentes o el uso de umbrales de vulnerabilidades. Se deben documentar los resultados de la identificación y que los revisen todas las partes interesadas. Los requisitos y los controles de SI deben reflejar el valor para el negocio de la información involucrada y el impacto potencialmente negativo sobre el negocio que podría resultar de la falta de seguridad adecuada.		

La organización debe integrar la identificación y la gestión de los requisitos de SI y los procesos asociados en las etapas tempranas de los proyectos de sistemas de información.

Los requisitos de SI también deben considerar:

a) El nivel de confianza requerido acerca de la supuesta identidad de los usuarios, para poder derivar los requisitos de autenticación de los usuarios.
b) Los procesos de provisión y autorización de accesos, para todos los usuarios de negocio, así como para los usuarios técnicos o con privilegios.
c) El informar a los usuarios y a los operadores sobre sus obligaciones y responsabilidades.
d) Las necesidades de protección requeridas para los activos involucrados, en particular con respecto a la disponibilidad, confidencialidad e integridad.
e) Los requisitos derivados de los procesos de negocios, tales como los requisitos de registro y monitoreo de las transacciones y de no repudio.
f) Los requisitos exigidos por otros controles de seguridad.

Si los productos son adquiridos, se debe seguir un proceso formal de prueba y adquisición. Los contratos con el proveedor deben abordar los requisitos de seguridad identificados. Cuando la funcionalidad de seguridad en el producto propuesto no satisface el requisito especificado, se debe reconsiderar el riesgo introducido y los controles asociados antes de adquirir el producto.

Se debe evaluar e implementar los lineamientos disponibles para la configuración de seguridad del producto alineados con la arquitectura final del software o servicio de dicho sistema.

Se deben a su vez definir los criterios para la aceptación de los productos, por ejemplo, en términos de su funcionalidad, lo cual asegurará que se cumplan los requisitos de seguridad identificados. Se deben evaluar los productos respecto de estos criterios antes de la adquisición. La organización debe revisar cualquier funcionalidad adicional para asegurar que no introduzca riesgos adicionales inaceptables.

ISO 27.001 A.14.1.1 [1] – ISO 27.001 14.1.1 [14]

GT1.2.2	Nivel D	F
Proceso de gestión de software		
Se deben establecer reglas para el desarrollo de software y de sistemas y se recomienda aplicarlas a los desarrollos dentro de la organización. El desarrollo seguro será un requisito para la construcción de un servicio, arquitectura, software y sistema seguros. Por lo que, la organización establecerá una política de desarrollo seguro, en función de los aspectos siguientes: a) La seguridad del entorno de desarrollo. b) Los lineamientos sobre la seguridad en el ciclo de vida de desarrollo de software. ▪ La seguridad en la metodología de desarrollo de software. ▪ Los lineamientos para la codificación segura en cada lenguaje de programación utilizado. c) Los requisitos de seguridad en la fase de diseño. d) Las verificaciones de seguridad dentro de los hitos del proyecto. e) Los repositorios seguros. f) La seguridad en el control de versiones. g) El conocimiento requerido en seguridad de las aplicaciones. h) La capacidad del desarrollador para evitar, encontrar y reparar vulnerabilidades.		
ISO 27.001 A.14.2.1 [1] – ISO 27.001 14.2.1 [14]		

GT1.2.3	Nivel D	F
Proceso de gestión de software		
La organización debe controlar los cambios a los sistemas dentro del ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios. Se deben documentar y hacer cumplir los procedimientos formales de control de cambios para asegurar la integridad del sistema, las aplicaciones y los productos, desde las etapas iniciales del desarrollo y a través de todos los esfuerzos de mantenimiento posteriores. Se debe seguir un proceso formal para la documentación, la especificación, las pruebas, el control de calidad y la		

implementación gestionada al introducir nuevos sistemas y cambios importantes en los sistemas existentes.

Este proceso debe incluir una evaluación de riesgos, un análisis del impacto de los cambios y una especificación de los controles de seguridad necesarios. Además, debe asegurar que los procedimientos de seguridad y de control existentes no se vean afectados, que los programadores de soporte sólo tengan acceso a aquellas partes del sistema necesarias para el desempeño de sus tareas, y que se obtengan un acuerdo y una aprobación formales para cualquier cambio.

Siempre que resulte factible, se deberán integrar los procedimientos de control de cambios operativos y de las aplicaciones. Los procedimientos de control de cambios deben incluir, pero sin limitarse a:

a) El mantenimiento de un registro de los niveles de autorización acordados.
b) La garantía de que los cambios son realizados por usuarios autorizados.
c) La revisión de los controles y los procedimientos de integridad para garantizar que no serán afectados por los cambios.
d) La identificación de todo el software, la información, las entidades de bases de datos y el hardware que requiera correcciones.
e) La identificación y la verificación de la seguridad del código crítico para minimizar la probabilidad de vulnerabilidades de seguridad conocidas.
f) La obtención de la aprobación formal para las propuestas detalladas antes de que comiencen las tareas.
g) La garantía de que los usuarios autorizados acepten los cambios antes de su implementación.
h) La garantía de que toda la documentación del sistema se encuentra actualizada cada vez que se completa un cambio, y de que se archiva o elimina la documentación vieja.
i) El mantenimiento de un control de versiones para todas las actualizaciones del software.
j) El mantenimiento de una pista para la auditoria de todas las solicitudes de cambio.
k) La garantía de que la documentación operativa y los procedimientos de usuarios se modifiquen según las necesidades, para que permanezcan apropiados.
l) La garantía de que la implementación de los cambios tenga lugar en el momento adecuado y no altere los procesos de negocio involucrados.

ISO 27.001 A.14.2.2 [1] – ISO 27.001 14.2.2 [14]

GT1.2.4	Nivel D	F
Proceso de gestión de software		
La organización deberá implementar procesos para controlar la instalación de software en los sistemas en producción, en función de los siguientes lineamientos: a) Los sistemas en producción sólo guardaran el código ejecutable aprobado, y no código en desarrollo o compiladores. b) Que se mantenga un registro para la auditoría de todas las actualizaciones de las librerías de programas en producción. c) Que se retengan las versiones previas del software de aplicaciones como una medida de contingencia. El software usado en sistemas en producción provisto por terceros siempre tenga soporte por parte del proveedor. La organización debe considerar los riesgos de depender de software que no tiene servicio de soporte. Solo se debe dar acceso físico o lógico a los proveedores, para casos de soporte, sólo cuando sea necesario y con aprobación de la gerencia. Se deben monitorear las actividades del proveedor.		
ISO 27.001 A.12.5.1 [1] - ISO 27.002 12.5.1 [14]		

GT1.2.5	Nivel C	F
Proceso de gestión de software		
Los sistemas de gestión de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad. Dicho sistema deberá: a) Forzar el uso de identificadores de usuarios y contraseñas individuales para mantener la trazabilidad. b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluya un procedimiento de confirmación para contemplar errores en su ingreso.		

c) Forzar la elección de contraseñas de calidad.
d) Obligar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión.
e) Forzar cambios de contraseñas a intervalos regulares y cuando sea necesario.
f) Mantener un registro de las contraseñas previamente utilizadas por el usuario y evite su reúso.
g) No mostrar las contraseñas en pantalla cuando se las ingresa.
h) Almacenar los archivos de contraseñas separados de los datos del sistema de aplicaciones.
i) Almacenar y transmitir las contraseñas en forma protegida.

En los casos que exista una autoridad independiente que asigne las contraseñas de usuario, los apartados b), d) y e) no serán aplicables.

ISO 27.001 A.9.4.3 [1] – ISO 27.001 9.4.3 [14]

GT1.2.6	Nivel C	F

Proceso de gestión de software

La organización deberá restringir el acceso al código fuente de los programas.

A su vez, deberá controlar estrictamente el acceso al código fuente de los programas y a los ítems asociados (tales como diseños, especificaciones, planes de verificación y planes de validación), para prevenir la introducción de funcionalidades no autorizadas y para evitar cambios no intencionales, así como mantener la confidencialidad de la propiedad intelectual.

Por otro lado, la organización deberá implementar los lineamientos siguientes:

a) Gestionar el código fuente de los programas y las librerías de fuentes de programas de acuerdo a procedimientos establecidos.
b) Que el personal de soporte no tenga acceso irrestricto a las librerías de fuentes de programas.
c) Que las actualizaciones de las librerías de fuentes de programas y los ítems asociados, y la distribución de las fuentes de los programas a los programadores se lleve a cabo después de recibir la autorización apropiada.
d) Que los listados de programas se almacenen en un entorno seguro.

e) Que se mantenga un registro de auditoría de todos los accesos a las librerías de fuentes de programas.
f) Que el mantenimiento y la copia de las librerías de fuentes de programas se encuentren sujetos a procedimientos estrictos de control de cambios.
g) Cuando sea posible, que las librerías de fuentes de programas no se mantengan en los entornos operativos.

Si se pretende publicar el código fuente de los programas, se recomienda considerar controles adicionales que ayuden a garantizar su integridad (por ejemplo, firma digital).

ISO 27.001 A.9.4.5 [1] – ISO 27.001 9.4.5 [14]

GT1.2.7	Nivel C	F

Proceso de gestión de software

La organización deberá separar los entornos de desarrollo, pruebas y producción para reducir los riesgos de accesos no autorizados o cambios en el entorno de producción. Para lo cual se deberán respetar los siguientes lineamientos:

a) Definir y documentar las reglas y el proceso para la transferencia de software del estado de desarrollo a producción.
b) Ejecutar el software de desarrollo y el software en producción en diferentes sistemas o procesadores y en diferentes dominios o directorios.
c) Probar los cambios a sistemas o aplicaciones en producción en un entorno de prueba o de simulación antes de aplicarlos al sistema en producción.
d) No realizar pruebas en sistemas en producción.
e) Que no se pueda acceder desde sistemas en producción, a los compiladores, editores y otras herramientas de desarrollo o utilitarios, cuando no sea necesario;
f) Que los usuarios utilicen distintos perfiles de usuario para los sistemas en producción y de prueba, y que los menús muestren mensajes de identificación apropiados para reducir el riesgo de error.
g) Que los datos sensibles no se copien al entorno de prueba del sistema excepto que se implementen controles equivalentes para el sistema de prueba.

ISO 27.001 A.12.1.4 [1] – ISO 27.001 12.1.4 [14]

GT1.2.8	Nivel C	F
Proceso de gestión de software		
La organización debe establecer y proteger adecuadamente los entornos de desarrollo para que los esfuerzos de desarrollo e integración cubran todo el ciclo de vida de desarrollo de los sistemas. Un entorno seguro de desarrollo incluye a la gente, los procesos y la tecnología asociados con el desarrollo y la integración de los sistemas. La organización debe evaluar los riesgos asociados con los esfuerzos de desarrollo de cada sistema en particular y establecer entornos seguros para el desarrollo de un sistema específico, considerando: a) La sensibilidad de los datos a procesar, almacenar e intercambiar por el sistema. b) Los requisitos internos y externos aplicables; por ejemplo: procedentes de reglamentaciones o políticas. c) Los controles de seguridad ya implementados por la organización que apoyan al desarrollo del sistema. d) La fiabilidad del personal que trabaja en el entorno. e) El grado de participación de terceras partes en el desarrollo del sistema. f) La necesidad de segregación entre distintos entornos de desarrollo. g) El control de acceso al entorno de desarrollo. h) El monitoreo de los cambios al entorno de desarrollo y al código almacenado en este. i) Los resguardos se almacenan en ubicaciones externas seguras. j) El control del movimiento de datos desde y hacia el entorno.		
ISO 27.001 A.14.2.6 [1] – ISO 27.001 14.2.6 [14]		

GT1.2.9	Nivel C	F
Proceso de gestión de software		
La organización debe supervisar y realizar el seguimiento de las actividades de desarrollo de los sistemas provistas por terceras partes.		

Cuando terceras partes proveen el desarrollo de los sistemas, se deben considerar los puntos siguientes a lo largo de toda la cadena de suministro externa de la organización: a) Los acuerdos de licencias, la propiedad de código y los derechos de propiedad intelectual relacionados con el contenido provisto por terceras partes. b) Los requisitos contractuales para las prácticas de seguridad en el diseño, la codificación y las pruebas. c) La provisión al desarrollador externo del modelo de amenazas aprobado. d) Las pruebas de aceptación para la calidad y la precisión de los entregables. e) La provisión de evidencia del uso de umbrales de seguridad, para establecer los niveles mínimos aceptables de seguridad y calidad de la privacidad. f) La provisión de evidencia de la aplicación de pruebas suficientes para protegerse contra la presencia de contenido malicioso, tanto intencional como no intencional, en la entrega. g) La provisión de evidencia de la aplicación de pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas. h) Los acuerdos de custodia a cargo de terceros. i) Los derechos contractuales para auditar los procesos y los controles de desarrollo. j) La documentación eficaz del entorno de desarrollo utilizado para crear los entregables. k) La organización retiene la responsabilidad por el cumplimiento de las leyes aplicables y la verificación de la eficiencia de los controles.
ISO 27.001 A.14.2.7 [1] – ISO 27.001 14.2.7 [14]

GT1.2.10	Nivel C	F
Proceso de gestión de software		
Se deberán realizar pruebas de las funcionalidades de seguridad durante el desarrollo. Se deberán a su vez, realizar pruebas de aceptación independientes (tanto para desarrollos internos como para los realizados por terceras partes) para asegurar que el sistema funcione de la manera esperada y solo de la manera esperada.		

La rigurosidad de las pruebas será proporcional a la importancia y la naturaleza del sistema.
ISO 27.001 A.14.2.8 [1] – ISO 27.001 14.2.8 [14]

GT1.2.11	Nivel C	F
Proceso de gestión de software		
Se deben establecer criterios y programas de pruebas de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas. Las pruebas de aceptación de los sistemas incluirán las pruebas de los requisitos de SI y del cumplimiento de las prácticas de seguridad en el desarrollo de sistemas. Las pruebas deberán realizarse en un entorno realista para asegurar que el sistema no vaya a introducir vulnerabilidades al entorno de la organización y que las pruebas son confiables.		
ISO 27.001 A.14.2.9 [1] – ISO 27.001 14.2.9 [14]		

GT1.2.12	Nivel C	F
Proceso de gestión de software		
La organización deberá proteger la información involucrada en servicios de aplicaciones que atraviesan redes públicas contra actividades fraudulentas, litigios contractuales y divulgaciones y modificaciones no autorizadas. Las consideraciones de SI para los servicios de aplicaciones sobre redes públicas incluirán lo siguiente: a) El nivel de confianza que cada parte requiere acerca de la supuesta identidad de las otras partes. b) Los procesos de autorización asociados con quien puede aprobar los contenidos de, emitir o firmar los documentos transaccionales clave.		

c) El aseguramiento que las partes intervinientes en la comunicación están completamente informadas de sus autorizaciones para la prestación o el uso del servicio.
d) La determinación y el cumplimiento de los requisitos de confidencialidad, integridad, prueba de envío y de recepción de documentos clave y el no repudio de los contratos; por ejemplo: asociados con los procesos de licitación y contratos.
e) El nivel de confianza requerido en la integridad de los documentos clave;
f) Los requisitos de protección de cualquier información confidencial.
g) La confidencialidad e integridad de las transacciones de cualquier orden, la información de pagos, los detalles de las direcciones de envío y la confirmación de recepción.
h) El grado apropiado para la verificación de la información de pago provista por un cliente.
i) La selección de la forma más apropiada para el procesamiento de pagos a fin de prevenir fraudes.
j) El nivel de protección requerido para mantener la confidencialidad e integridad de la información de los pedidos.
k) Evitar la pérdida o la duplicación de la información de transacciones.
l) Las obligaciones asociadas con cualquier transacción fraudulenta.
m) Los requisitos impuestos por los seguros.

ISO 27.001 A.14.1.2 [1] – ISO 27.001 14.1.2 [14]

GT1.2.13	Nivel C	F

Proceso de gestión de software

Se deberá proteger la información involucrada en las transacciones de los servicios de aplicaciones para prevenir transmisiones incompletas, ruteo erróneo, alteración no autorizada de los mensajes, divulgación no autorizada, duplicación o repetición no autorizadas de los mensajes.

Las consideraciones de SI para las transacciones de servicios de aplicaciones incluirán lo siguiente:

a) El uso de firmas electrónicas para cada una de las partes involucradas en la transacción.

b) Todos los aspectos de la transacción.
c) Que los caminos de las comunicaciones entre todas las partes involucradas estén cifrados.
d) Que se aseguren los protocolos utilizados para la comunicación entre todas las partes involucradas.
e) Que se asegure que el almacenamiento de los detalles de las transacciones esté ubicado fuera de cualquier ambiente de acceso público (por ejemplo, sobre una plataforma de almacenamiento existente en la intranet de la organización), y no mantenido y expuesto en un medio con acceso directo desde internet.
f) Que cuando se utilice una autoridad confiable, la seguridad esté integrada y embebida a través de todo el proceso de gestión de los certificados/firmas, de punta a punta.

ISO 27.001 A.14.1.3 [1] – ISO 27.001 14.1.3 [14]

GT1.2.14	Nivel C	F

Proceso de gestión de software

Cuando se cambian los sistemas en producción, se deberán revisar y probar las aplicaciones críticas del negocio para asegurar que no se produzca un impacto adverso en las operaciones o en la seguridad de la organización.

Dicho proceso deberá cubrir:

a) La revisión de los procedimientos de integridad y control de las aplicaciones, para garantizar que éstos no hayan sido afectados por los cambios en las plataformas operativas.
b) La garantía de que se notifiquen a tiempo los cambios en las plataformas operativas, para permitir que se lleven a cabo pruebas y revisiones apropiadas antes de la implementación.
c) La garantía de que se realicen los cambios apropiados a los planes de continuidad del negocio.

ISO 27.001 A.14.2.3 [1] – ISO 27.001 14.2.3 [14]

GT1.2.15	Nivel C	F
Proceso de gestión de software		
Se deberán desalentar las modificaciones en los paquetes de software, limitarlas a los cambios necesarios y controlar estrictamente todos los cambios. En la medida de lo posible y lo factible, los paquetes de software suministrados por proveedores se utilizarán sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberán considerar los puntos siguientes: a) El riesgo de que los controles y los procesos de integridad incorporados se vean afectados. b) Si es necesario contar con el consentimiento del proveedor. c) La posibilidad de obtener los cambios requeridos a través del proveedor en forma de actualizaciones normales del programa. d) El impacto que se produciría si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios. e) La compatibilidad con otro software que esté en uso. Si los cambios se consideran necesarios, se debe retener el software original y aplicar los cambios a una copia designada. Se deberá implementar un proceso de gestión de las actualizaciones de software para garantizar que se instalen los últimos parches aprobados y las actualizaciones de aplicaciones para todo el software autorizado. A su vez, se debe probar y documentar completamente todos los cambios, de manera que puedan aplicarse nuevamente, de ser necesario, a futuras actualizaciones del software. En caso de ser necesario, probar y validar las modificaciones por un ente evaluador independiente.		
ISO 27.001 A.14.2.4 [1] – ISO 27.001 14.2.4 [14]		

GT1.2.16	Nivel C	F
Proceso de gestión de software		
Se deberán establecer, documentar, mantener y aplicar los principios de seguridad para el desarrollo de sistemas seguros, en la implementación de sistemas de información.		

Se deben establecer, documentar y aplicar los procedimientos para el desarrollo de sistemas de información seguros, basados en los principios de seguridad para el desarrollo de sistemas, en todas las actividades internas de desarrollo de sistemas de información. La seguridad en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología) se diseñará, balanceando las necesidades de SI contra las necesidades de accesibilidad. Se recomienda analizar la nueva tecnología en busca de riesgos y revisar el diseño en función de los patrones de ata-que conocidos. Se deben revisar periódicamente estos principios y los procedimientos de desarrollo de sistemas establecidos para garantizar que contribuyan eficazmente a mejorar los estándares de seguridad dentro del proceso de desarrollo. También se deberá revisarlos periódicamente para asegurar que permanezcan actualizados para poder contrarrestar cualquier amenaza potencial nueva. y que permanezcan aplicables a los avances tecnológicos y a las soluciones que se están utilizando. Cuando corresponda, se aplicarán los principios de seguridad en el desarrollo de los sistemas de información provistos por terceros, a través de contratos u otros acuerdos legales entre la organización y el proveedor. La organización confirmará que el rigor de los principios de seguridad en el desarrollo de sistemas del proveedor sea comparable con el suyo.
ISO 27.001 A.14.2.5 [1] – ISO 27.001 14.2.5 [14]

GT1.2.17	Nivel C	F
Proceso de gestión de software		
Se deberá seleccionar cuidadosamente, proteger y controlar los datos de prueba. Se debe evitar el uso de datos operativos que contengan información personal o cualquier otra información confidencial con el propósito de pruebas. Si la información personal u otra información confidencial se utilizan con propósito de pruebas, se recomienda proteger todos los detalles y contenido sensibles removiéndolos o modificándolos.		

Se deberán aplicar los lineamientos siguientes para proteger los datos operativos cuando se los utiliza con propósitos de prueba:

a) Que los procedimientos de control de accesos, los cuales aplican a las aplicaciones en sistemas en producción, también se apliquen a las aplicaciones en sistemas de prueba.
b) Que se autorice por separado cada vez que se copie la información operativa al entorno de prueba.
c) Que se borre la información operativa del entorno de prueba inmediatamente después de finalizar las pruebas.
d) Que se registre la copia y el uso de la información operativa para proporcionar pistas para la auditoría.

ISO 27.001 A.14.3.1 [1] – ISO 27.001 14.3.1 [14]

GT1.2.18	Nivel C	F

Proceso de gestión de software

A fin de controlar los cambios en el software en los sistemas en producción, se deberán considerar los lineamientos siguientes:

a) Que la actualización del software, las aplicaciones y las librerías de programas en producción, sólo la realicen administradores capacitados bajo autorización apropiada de la gerencia.
b) Que el software de aplicaciones y del sistema en producción se implemente luego de probarlo extensiva y exitosamente; que las pruebas incluyan usabilidad, seguridad, efectos sobre otros sistemas y cuan intuitivo es para el usuario, y que se lleven a cabo en sistemas separados.
c) Que se use un sistema de control de la configuración para mantener el control de todo el software implementado, así como de la documentación del sistema.
d) Que se establezca una estrategia de vuelta atrás antes de implementar los cambios.
e) Que las versiones viejas del software se archiven, junto con toda la información, los parámetros, los procedimientos, los detalles de configuración, y el software de soporte requeridos durante todo el tiempo que se retengan los datos archivados.

Cualquier decisión de actualizar una nueva versión deberá tener en cuenta los requisitos del negocio respecto del cambio y de la seguridad de la versión.
ISO 27.002 12.5.1 [14]

GT1.2.19	Nivel B	F
Proceso de gestión de software		
El entorno de desarrollo deberá simular las mismas condiciones del entorno de producción. No se podrán utilizar datos reales de los sistemas en producción para realizar pruebas a nuevos desarrollos de software.		

[Página dejada en blanco intencionalmente]

GT2 GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

GT2.1 Lineamientos de Gestión & Eficiencia operativa

Objetivo Establecer los fundamentos y lineamientos de gestión y eficiencia operativa para el manejo de los centros de cómputos de la organización. Dichos lineamientos se encuentran estrechamente relacionados con aquellos relativos a la continuidad de las operaciones.

GT2.1.1	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
La organización deberá garantizar que existe suficiente capacidad para satisfacer las necesidades de uso de su centro de cómputos. *Debemos recordar que el concepto de centro de cómputos hace referencia tanto a centros de cómputos propios dentro de las instalaciones de la organización como aquellos alojados en un tercero o totalmente tercerizados a un tercero.*		
TIER Standard 2.1.1 [25]		

GT2.1.2	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá realizar mantenimiento preventivo a todos los dispositivos de hardware que componen el centro de cómputos.		
TIER Standard 2.1.3 [25]		

GT2.1.3	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Las instalaciones de gestión de condiciones ambientales del centro de cómputos (temperatura, altitud, humedad, entre otras) deberán poder hacer frente a las condiciones más adversas probables para el sitio geográfico en donde se encuentra. *Por ejemplo, deberá poder soportar las temperaturas históricas más altas registradas en esa zona geográfica durante el verano.*		
TIER Standard 2.6 [25]		

GT2.1.4	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá: a) Un equipo de enfriamiento dedicado que no sea desactivado fuera de las horas normales de oficina. b) Equipamiento UPS con capacidad para el total del equipamiento del centro de cómputos. c) Poseer un ambiente superior al de una mera oficina u otro tipo de área u oficina dentro de las instalaciones de la organización. d) Poseer un generador de energía eléctrica. El mimo podrá tener un limitante de n horas de operación concurrente.		

Se recomienda implementar UPS en los dispositivos que se encuentran fuera del centro de cómputos.
TIER Standard 3.3.1 [25]

GT2.1.5	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
La disponibilidad anual del centro de cómputos no podrá ser menor al 95%.		
TIER Standard 3.1 [25]		

GT2.1.6	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá asignar personal (propio, contratado o de terceros) part-time o full-time para el monitoreo y gestión de las operaciones del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.7	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
El personal deberá contar con las licencias/certificaciones necesarias requeridas por los diferentes niveles de gobierno y legislación correspondientes a la ubicación geografía del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.8	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con una estructura formal definida que abarque la organización jerárquica y de trabajo de todo el personal (propio, contratado o de terceros) afectados al monitoreo, gestión, operación y mantenimiento del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.9	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
El porcentaje de cumplimiento de las tareas, actividades, procesos y proyectos vinculados al centro de cómputos no podrá ser menor al 90%.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.10	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con un registro de todos los proveedores de los sistemas, equipamientos y herramientas vinculadas al centro de cómputos, tanto para trabajos y contacto de emergencia como generales. Dicho registro deberá encontrarse adecuadamente disponible para su consulta.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.11	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
El área y el piso destinados al centro de cómputos deberá permanecer libre de residuos, basura, escombros y elementos no imprescindibles para la operación de este.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.12	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con un sistema de gestión de las actividades de mantenimiento vinculadas al centro de cómputos. Dicho sistema podrá encontrarse basado en papel o bien ser completamente digital.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.13	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con un programa de mantenimiento programado que documente y registre todas las acciones de mantenimiento, sus fechas límites y el registro de su concreción.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.14	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberán realizar capacitaciones del formato "*on-site*" (en el sitio, simulando una actividad de trabajo en el verdadero entorno) sobre los sistemas (de los		

cuales serán responsables de operar y mantener) y de las reglas y lineamientos que enmarquen su trabajo dentro del centro de cómputos, previo al ingreso del personal´.
TIER Standard 4 Tabla 1.3 [26]

GT2.1.15	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberán realizar capacitaciones regulares sobre: a) Los accesos al centro de cómputos. b) Las reglas de trabajo dentro del centro de cómputos. c) Los procesos para el personal de mantenimiento y limpieza dentro del centro de cómputos.		
TIER Standard 4 Tabla 1.3 [26]		

GT2.1.16	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
La siguiente documentación deberá encontrarse actualizada y adecuadamente disponible: a) Planos del centro de cómputos. b) Documentación sobre la operación y mantenimiento del centro de cómputos. c) Reportes comisionados vinculados al centro de cómputos. d) Documentos de garantía. e) Estudios (eléctrico, estructural, de suelo, mecánico, de circuitos, etc.) centro de cómputos. f) Secuencias de operación adecuadamente documentadas.		
TIER Standard 4 Tabla 1.4 [26]		

GT2.1.17	Nivel E	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá diseñar, mantener e implementar el proceso de instalación y remoción del requipamiento del centro de cómputos.		
TIER Standard 4 Tabla 1.4 [26]		

GT2.1.18	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá contar con componentes redundantes. Deberá poseer al menos un componente más de cada uno necesario (N+1). *El presente requerimiento no aplica al canal de alimentación eléctrica de dichos dispositivos. El mismo es requisito del nivel de madurez "C".*		
TIER Standard 2.2.1 [25]		

GT2.1.19	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Los componentes redundantes del centro de cómputos deberán poder ser removidos sin necesidad de desactivar ningún equipo, dentro del marco del mantenimiento preventivo programado de dichos componentes.		
TIER Standard 2.2.2 [25]		

GT2.1.20	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá implementar UPS en los dispositivos que se encuentran fuera del centro de cómputos.		

GT2.1.21	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá: a) Poseer un equipo de enfriamiento dedicado redundante. b) Poseer un equipo de abastecimiento de energía critica redundante. c) Poseer UPS redundantes. d) Poseer equipos de rechazo de calor.		
TIER Standard 3.3.2 [25]		

GT2.1.22	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
La disponibilidad anual del centro de cómputos no podrá ser menor al 99%.		
TIER Standard 3.1 [25]		

GT2.1.23	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá asignar personal (propio, contratado o de terceros) por al menos un turno de 8 horas diarias durante los días hábiles (lunes a viernes) para el monitoreo y gestión de las operaciones del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.24	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberán establecer procesos de escalamiento para el personal asignado a sistemas y equipamiento clasificado con sensibilidad CRÍTICA.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.25	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberán realizar capacitaciones sobre los procesos y equipamiento específicos del centro de cómputos. Dichas capacitaciones deberán ser adecuadamente documentadas.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.26	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Cada rol afectado a la operación, monitoreo y mantenimiento del centro de cómputos deberá contar con su descripción de tareas y trabajo adecuadamente documentada y disponible para su consulta en todo momento.		

TIER Standard 4 Tabla 1.1 [26]

GT2.1.27	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá registrar todas las fallas e interrupciones en el servicio y disponibilidad del centro de cómputos, documentando: a) Fecha y hora. b) infraestructura, equipamiento, sistemas y dispositivos involucrados. c) Resultado del análisis de causa raíz. d) Descripción de las lecciones aprendidas.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.28	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberán tener establecidos acuerdos de nivel de servicio (SLAs por sus siglas en ingles) para todos los proveedores críticos del equipamiento, componentes, sistemas, dispositivos y herramientas del centro de cómputos. Dichos acuerdos deberán detallar: a) Alcance del trabajo. b) Tiempos de respuesta. c) Responsabilidades de ambas partes. d) Puntos de contacto. e) Proceso de contacto. f) Clausulas de salida. g) Cronograma de coordinación de actividades y procesos.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.29	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Los lineamientos de gestión de proyectos deberán comprender las recomendaciones de mantenimiento de los proveedores.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.30	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Los centros de cómputos deberán encontrarse libres de combustibles, equipamiento de limpieza, cajas de distribución/envió, objetos personales o cualquier otro elemento que no sea indispensable para la operación, mantenimiento y gestión del centro de cómputos.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.31	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá mantener un registro de todo el equipamiento vinculado al centro de cómputos, detallando: a) Modelo. b) Marca. c) Año de fabricación. d) Año de instalación. e) Especificaciones operativas. f) Información de garantía.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.32	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer espacio suficiente para el desarrollo seguro de las actividades de mantenimiento de este.		
TIER Standard 4 Tabla 2.2 [26]		

GT2.1.33	Nivel D	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá diseñar, mantener actualizado e implementar un plan maestro del centro de cómputos.		
TIER Standard 4 Tabla 1.4 [26]		

GT2.1.34	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá contener múltiples flujos de distribución de energía. Configura el extra descripto en el requerimiento GT2.1.4. No obstante, solo se requiere que uno de dichos flujos alimente al equipamiento en un determinado momento. En otras palabras, no es necesario que los flujos de energía alimenten a los dispositivos en simultáneo. *El centro de cómputos debe poseer un flujo de energía activo y otro alternativo. Esto puede lograrse con la instalación de un generador de energía eléctrica. A su vez, la alimentación de energía deberá realizarse desde dos compañías diferentes o bien desde dos subestaciones diferentes de la misma compañía de suministro eléctrico.* El generador de energía, y todos sus elementos y componentes de soporte, deberán ser tolerantes a fallas y/o cumplir con los lineamientos del mantenimiento concurrente. A su vez, el generador de energía no deberá poseer un límite de n horas de operación consecutiva.		

GT2.1.4
TIER Standard 2.3.1, 2.5 y 2.7 [25]

GT2.1.35	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Todo el equipamiento de TI deberá poseer al menos dos alimentaciones de energía en función de las especificaciones de tolerancia a fallas de energía del Uptime Institute. De no cumplir con dichas especificaciones deberán instalarse dispositivos de transferencia en los equipamientos.		
TIER Standard 2.3.1 [25]		

GT2.1.36	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Cualquier componente de capacidad o de distribución de energía del centro de cómputos deberá poder ser removido, en función del mantenimiento programado, sin impactar en el funcionamiento de ninguno de los equipamientos del dentro de cómputos.		
TIER Standard 2.3.2 [25]		

GT2.1.37	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
La capacidad instalada permanente del centro de cómputos debe poder satisfacer la demanda aun cuando los componentes redundantes son retirados de servicio por cualquier motivo.		
TIER Standard 2.3.2 [25]		

GT2.1.38	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El mantenimiento preventivo programado puede realizarse sin desactivar la capacidad instalada permanente del centro de cómputos, ya que pueden utilizarse tanto los componentes redundantes como los flujos de distribución de energía redundantes. *El centro de cómputos deberá ser compatible con la práctica de mantenimiento concurrente.*		
TIER Standard 2.3.3 y 2.7 [25]		

GT2.1.39	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
La disponibilidad anual del centro de cómputos no podrá ser menor al 99,98%.		
TIER Standard 3.1 [25]		

GT2.1.40	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá: a) Poseer flujos de distribución de energía redundantes. b) Cumplir con los lineamientos del mantenimiento concurrente (todo componente o sistema tanto de TI como de infraestructura del centro de cómputos podrá ser desconectado para el mantenimiento preventivo programado sin impactar en el funcionamiento del centro de cómputos). c) Poseer válvulas de aislación. d) Poseer un mecanismo antincendios adecuado. Preferentemente basado en el conocido sistema FM-200.		

TIER Standard 3.3.3 [25]

GT2.1.41	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá poseer una presencia de personal 24x7 para el monitoreo y gestión de las operaciones del centro de cómputos. A su vez, se deberá contar con al menos un recurso full-time calificado y especializado en el monitoreo y gestión de las operaciones del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.42	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El personal asignado al centro de cómputos deberá contar con capacitación formal y completa sobre las siguientes temáticas: a) Configuración del centro de cómputos. b) Operación del centro de cómputos. c) Procedimientos de emergencia. d) Procesos, políticas y procedimientos de todo nivel vinculados a la operación y mantenimiento del centro de cómputos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.43	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con una matriz RACI que detalle todas las actividades y procesos (junto con sus responsables) vinculados a la operación, mantenimiento y gestión del centro de cómputos.		

TIER Standard 4 Tabla 1.1 [26]

GT2.1.44	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El total numérico del personal (propio, contratado o de terceros) afectado a las tareas del centro de cómputos deberá como mínimo coincidir con la sumatoria de los requerimientos mínimos de personal de cada uno de los turnos.		
TIER Standard 4 Tabla 1.1 [26]		

GT2.1.45	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con procesos formales documentados sobre: a) El intercambio de uso entre el equipamiento redundante. b) La calidad de la gestión de proyectos. c) El adecuado cumplimiento de los proyectos. d) Las actividades de mantenimiento preventivo. e) Gestión de contacto con proveedores (incluyendo los puntos de contacto para el mantenimiento técnico pre acordado). f) La búsqueda de la causa raíz de errores, fallas y disrupciones del servicio. g) La identificación de lecciones aprendidas, en función de los resultados de f). h) El diseño, implementación y mantenimiento de acciones correctivas. i) El planeamiento, cronograma y gestión de presupuesto del ciclo de vida de los componentes (sistemas, equipamiento, herramientas y demás) de la infraestructura del centro de cómputos (desde su desarrollo, obtención o adquisición hasta su reemplazo). *Todos los procesos detallados en el presente requerimiento tendrán alcance restringido al centro de cómputos y todas las partes interesadas vinculadas al mismo.*		

TIER Standard 4 Tabla 1.2 [26]

GT2.1.46	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá monitorear y almacenar datos, estadísticas e información histórico sobre las siguientes actividades/procesos vinculadas al centro de cómputos: a) Gestión de proyectos (los proyectos en sí, sus mecanismos de desarrollo y ejecución, y responsabilidades). b) Gestión del equipamiento. c) Actividades de mantenimiento. d) Requerimientos de calibración de equipos. e) Puntos de repedido y de almacenamiento crítico (gestión del inventario de herramientas, dispositivos y hardware).		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.47	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá contar con un porcentaje de cumplimiento del alcance y objetivos de los proyectos vinculados al centro de cómputos del 100%.		
TIER Standard 4 Tabla 1.2 [26]		

GT2.1.48	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá encontrarse diseñado en forma tal que facilite futuros aumentos incrementales en capacidad, energía, espacio y enfriamiento		

para que solo requiere un esfuerzo razonable para tales incrementos y con un mínimo riesgo a la operatoria y capacidad actual del dentro de cómputos.
TIER Standard 4 Tabla 2.3 [26]

GT2.1.49	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer unidades de extensión o de capacidad para uso futuro o temporal.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.50	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer sistemas de soporte mecánico que se enfoquen en extender la vida de la infraestructura de este y, a su vez, de protegerla.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.51	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer sistemas mecánicos que faciliten las operaciones de este.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.52	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El equipamiento del centro de cómputos deberá encontrarse adecuadamente inventariado y etiquetado en todo momento. A su vez, el equipamiento deberá ser de tamaño estándar.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.53	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer sistemas eléctricos instalados que faciliten la operación de este.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.54	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá poseer un acceso específico para la entrada/salida, montaje e instalación de equipamientos y componentes de gran tamaño. Dicho acceso deberá facilitar la rápida remoción del equipamiento/material y su consecuente reemplazo.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.55	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
Se deberá diseñar, implementar y mantener un proceso para el uso alternativo del equipamiento de infraestructura del centro de cómputos como parte del programa de mantenimiento de este.		
TIER Standard 4 Tabla 2.3 [26]		

GT2.1.56	Nivel C	F
Macroproceso de gestión de la infraestructura de TI		
El centro de cómputos deberá: a) Poseer un control de acceso (como a su vez las instalaciones donde se encuentra ubicado). b) Poseer espacio adecuado para las tareas de mantenimiento, reabastecimiento, almacenamiento de herramientas y equipamiento, entre otras actividades relativas a su operatoria y mantenimiento. c) Poseer sistemas integrados de testeo operacional (ISOT por sus siglas en ingles).		
TIER Standard 4 Tabla 2.1 y 2.4 [26]		

[Página dejada en blanco intencionalmente]

GESTIÓN DE RECURSOS HUMANOS

El objetivo primordial del presente subsistema comprende el establecimiento de los lineamientos de Seguridad de la Información vinculados al actor más importante y a la primera línea de defensa de la organización en materia de seguridad: su personal (tanto sea propio, contratado o de terceras partes).

Se enfoca principalmente en establecer ciertos lineamientos estratégicos que direccionarán el accionar de la organización hacia el involucramiento del recurso humano y su adecuada, periódica y efectiva formación.

RH1 Gestión de la seguridad de los RRHH

RH1.1 "Antes y después del empleo" [1]

RH1.2 "Durante el empleo" [1]

RH2 Programa de toma de Conciencia, Entrenamiento y Difusión

RH2.1 Metodología de Conciencia, Entrenamiento y Difusión

RH1 GESTIÓN DE LA SEGURIDAD DE LOS RRHH

RH1.1 "Antes y después del empleo" [1]

Objetivo Establecer los lineamientos de Seguridad de la Información que la organización deberá tener en cuenta previamente a la contratación de personal (tanto sea contratista, de tercera parte o propio de la organización).

RH1.1.1	Nivel D	F
Subproceso de antecedentes		
La organización deberá realizar la verificación de antecedentes de todos los candidatos para el empleo (sean futuros empleados propios, contratistas o de terceras partes) de acuerdo con las leyes, regulaciones y reglas éticas pertinentes. Se recomienda que dicha verificación sea proporcional a los requisitos del negocio, la clasificación de sensibilidad de la información a ser accedida y los riesgos de seguridad percibidos. Se deberá establecer el proceso para la notificación a seguir si la investigación no se completa o si los resultados causan duda o preocupación.		
ISO 27.001 A.7.1.1 [1] – ISO 27.002 7.1.1 [14]		

RH1.1.2	Nivel C	F
Subproceso de antecedentes		
La verificación de antecedentes de todos los candidatos para el empleo deberá al menos considerar lo siguiente: a) La disponibilidad de referencias satisfactorias de carácter. b) La verificación (tanto para completitud y precisión) completa del currículum vitae del aspirante. c) La confirmación de las calificaciones académicas y profesionales presentadas, por parte de dichas organizaciones y un sistema de información centralizado (tanto sea estatal o privado). d) La verificación independiente de la identidad (a través de un pasaporte o documento similar). e) Verificaciones crediticias y de antecedentes criminales. Se deberán realizar verificaciones más detalladas para aquellos candidatos que asuman una posición (ya sea una incorporación inicial o una promoción) que involucra acceso a las instalaciones de procesamiento de la información o acceso a información clasificada con sensibilidad CRÍTICA o ALTA. Se les deberá informar a los candidatos de antemano acerca de las actividades de investigación de antecedentes.		
ISO 27.002 7.1.1 [14]		

RH1.1.3	Nivel C	F
Subproceso de gestión de contratos		
Los contratos laborales con empleados, contratistas y terceras partes deberán establecer sus responsabilidades y las de la organización para con la SI. Todos los empleados y contratistas a quienes se les otorgue acceso a la información de la organización (o bajo custodia de está) deberán firmar un acuerdo de confidencialidad antes de darles acceso a las instalaciones de procesamiento de la información.		

ISO 27.001 A.7.1.2 [1] – ISO 27.002 7.1.2 [14]

RH1.1.4	Nivel C	F
Subproceso de gestión de contratos		
Las obligaciones contractuales para los empleados y contratistas deberán reflejar: a) Las responsabilidades y derechos legales de empleados y contratistas. b) Las responsabilidades para la clasificación de la información y para la gestión de información y otros activos de la organización asociados con información, instalaciones de procesamiento de información y servicios de información manejados por el empleado o contratista. c) Las responsabilidades del empleado o contratista para el manejo de la información recibida de otras organizaciones o terceras partes. d) Las acciones a ser llevadas a cabo si el empleado o contratista no cumple los requisitos de seguridad de la organización.		
ISO 27.002 7.1.2 [14]		

RH1.1.5	Nivel C	F
Subproceso de estructura de RRHH		
Se deberán comunicar los roles y responsabilidades de la SI a los candidatos al puesto durante el proceso previo al empleo. La organización debe asegurarse que los empleados y contratistas estén de acuerdo con los términos y condiciones concernientes a la SI, adecuados a la naturaleza y extensión del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información. Las responsabilidades contenidas dentro de los términos y condiciones del empleo deberán continuar por un período definido de tiempo luego de la finalización la relación laboral.		

ISO 27.002 7.1.2 [14]

RH1.1.6	Nivel C	F
Subproceso de gestión de obligaciones		
La organización deberá definir, comunicar y hacer cumplir, al empleado o contratista, las responsabilidades y las obligaciones relativas a la SI que continúan vigentes luego de la desvinculación o cambio de puesto. La comunicación de las responsabilidades de desvinculación debe incluir los requisitos de seguridad y las responsabilidades legales que continúan vigentes y, cuando corresponda, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad y los términos y condiciones de empleo que continúan por un período definido de tiempo luego de la finalización del trabajo del empleado o contratista. Las responsabilidades y obligaciones que siguen siendo válidas luego de la terminación del empleo deben estar incluidas en los términos y condiciones de empleo con el empleado o contratista. A su vez, se deberá informar a los empleados, clientes o contratistas acerca de los cambios de personal y de operaciones El área de RRHH deberá encargarse de la ejecución del presente requerimiento, en conjunto con el responsable jerárquico de quien se está desvinculando.		
ISO 27.001 A.7.3.1 [1] – ISO 27.002 7.3.1 [14]		

RH1.1.7	Nivel C	F
Subproceso de gestión de obligaciones		
Se recomienda que los cambios de responsabilidad o de empleo se gestionen como la terminación de la responsabilidad o del empleo actual junto con el inicio de la responsabilidad o del empleo nuevo.		
ISO 27.002 7.3.1 [14]		

RH1.1.8	Nivel C	F
Subproceso de gestión de obligaciones		
Se deberán establecer acuerdos de confidencialidad previo al ingreso al puesto de trabajo. Dicho acuerdo de confidencialidad deberá durar por un tiempo determinado o indeterminado luego de la recisión del contrato.		
ISO 27.002 7.3.1 [14]		

RH1.1.9	Nivel B	F
Subproceso de gestión de RRHH		
Cuando se contrata a una persona para un rol específico en SI, la organización deberá asegurarse que el candidato: a) Tenga la competencia necesaria para desempeñarse en el rol relacionado con la seguridad. b) Sea confiable para asumir ese rol, especialmente si el rol es crítico para la organización. La organización deberá establecer un proceso que defina criterios y limitaciones para la revisión de las verificaciones de los candidatos.		
ISO 27.002 7.1.1 [14]		

RH1 GESTIÓN DE LA SEGURIDAD DE LOS RRHH

RH1.2 "Durante el empleo" [1]

Objetivo Establecer los lineamientos de Seguridad de la Información que la organización deberá tener en cuenta durante la ejecución del contrato del personal (tanto sea contratista, de tercera parte o propio de la organización).

RH1.2.1	Nivel E	F
La dirección ejecutiva de la organización deberá requerir a todos los empleados, contratistas y usuarios de terceras partes que apliquen la SI de acuerdo con todas las políticas y procesos establecidos por la organización dentro de su Sistema de Mejora Continua. La dirección ejecutiva de la organización debe demostrar su apoyo a las políticas, los procedimientos y controles de la SI, y actuar como el ejemplo a seguir. A su vez, la organización deberá proporcionar un canal anónimo para informar acerca de violaciones a las políticas o los procedimientos de SI.		
ISO 27.001 A.7.2.1 [1] – ISO 27.002 7.2.1 [14]		

RH1.2.2	Nivel E	F
La organización deberá implementar un proceso disciplinario formal y comunicado para sancionar a los empleados que hayan cometido una violación a la SI. Dicho proceso disciplinario no deberá iniciarse sin la previa verificación de que haya ocurrido una violación a la SI. El proceso disciplinario formal deberá asegurar un tratamiento correcto y justo de los empleados de los que se sospecha que hayan cometido violaciones a la SI. Debe proporcionar una respuesta progresiva, la cual tenga en cuenta factores como la naturaleza y la gravedad de la violación y su impacto en el negocio, si es la primera infracción o si es reiterada, si el infractor ha sido o no apropiadamente capacitado, la legislación pertinente, los contratos de negocio, y cualquier otro factor que se requiera. Debe ser utilizado como un disuasivo para prevenir que los empleados, contratistas y terceras partes violen las políticas y los procesos de SI de la organización y cualquier otra violación a la SI. Violaciones intencionales requerirán acciones inmediatas. *El proceso disciplinario también puede ser utilizado como una motivación o un incentivo si se definen sanciones positivas para conductas notables con respecto a la SI.*		
ISO 27.001 A.7.2.3 [1] – ISO 27.002 7.2.3 [14]		

RH1.2.3	Nivel D	F
La organización deberá realizar capacitaciones periódicas y continuas sobre todos los lineamientos, políticas y procesos de SI que conformen el Sistema de Mejora Continua de la organización.		

RH1.2.4	Nivel D	F
Los empleados, contratistas y terceras partes deberán: a) Estar adecuadamente informados sobre sus roles y responsabilidades respecto de la SI antes de que se les otorgue acceso a información confidencial o a los sistemas de información. b) Estar motivados para cumplir con las políticas de SI de la organización. c) Alcanzar un nivel de conciencia sobre la SI acorde a sus roles y responsabilidades dentro de la organización.		
ISO 27.002 7.2.1 [14]		

RH1.2.5	Nivel C	F
Todos los empleados de la organización y, cuando sea pertinente los contratistas y las terceras partes vinculadas, deberán recibir una concientización, educación y capacitación continuas apropiadas, y actualizaciones regulares en las políticas y procesos organizacionales, que sean pertinentes a su tarea.		
ISO 27.001 A.7.2.2 [1]		

RH1.2.6	Nivel C	F
Los empleados, contratistas y terceras partes deberán: a) Estar provistos de lineamientos para establecer las expectativas de SI correspondientes a su rol dentro de la organización. b) Cumplir con los términos y las condiciones del empleo, los cuales incluyen las políticas de SI de la organización y los métodos adecuados de trabajo.		

c) Seguir teniendo las habilidades y calificaciones adecuadas, y reciban capacitación periódicamente.
ISO 27.002 7.2.1 [14]

RH2 PROGRAMA DE TOMA DE CONCIENCIA DE SI

RH2.1 Metodología de Conciencia, Entrenamiento y Difusión

Objetivo Establecer los fundamentos de la metodología de toma de conciencia, entrenamiento y difusión de la Seguridad de la Información unificada que tenga como alcance a todo el personal, contratistas y usuarios de terceras partes vinculados a la organización

RH2.1.1	Nivel E	F
Macroproceso de formación		
La organización deberá realizar campañas ocasionales de concientización de SI en función de las amenazas priorizadas por la ejecución del proceso de gestión de riesgos.		

RH2.1.2	Nivel D	F
Macroproceso de formación		
Todas las partes interesadas internas de la organización deberán ser conscientes de: a) La Política de SI.		

b) Su contribución a la eficacia del Sistema de Mejora Continua de la SI de la organización. c) Las implicancias de no cumplir con los requerimientos y lineamientos del Sistema de Mejora Continua de la SI de la organización y cualquiera de sus políticas, procesos y procedimientos asociados.
ISO 27.001 7.3 [1]

RH2.1.3	Nivel D	F
Macroproceso de formación		
La organización deberá: a) Determinar la competencia necesaria de las personas bajo su control que realicen actividades que afecten el desempeño de la organización en SI. b) Asegurar que todas las personas incluidas en a) sean competentes en función de requerimientos de educación, capacitación y experiencia apropiados. c) Realizar acciones con el objetivo de colaborar que las personas incluidas en a) adquieran la competencia necesaria. d) Realizar acciones con el objetivo de adquirir la competencia necesaria (por ejemplo: a través de la implementación de capacitaciones, asignación de tutores, la reasignación de empleados o la incorporación a la organización de personas competentes). e) Evaluar la eficacia de las acciones establecidas en c). f) Conservar información documentada apropiada como evidencia de la competencia de las personas incluidas en a).		
ISO 27.001 7.2 [1]		

RH2.1.4	Nivel D	F
Macroproceso de formación		
Se deberá solicitar a los usuarios que sigan las prácticas de la organización referidas al uso de la información secreta de autenticación.		

La organización deberá capacitar a los usuarios (propios, contratistas y de terceras partes) sobre:

a) No usar la misma contraseña para propósitos de negocio y personales.
b) No compartir la información secreta de autenticación.
c) Cambiar la información secreta de autenticación ante cualquier indicio de su posible compromiso.
d) La prohibición de mantener un registro de la información secreta de autenticación, a menos que se cuente con la debida autorización y se pueda almacenar de forma segura mediante un método de almacenamiento apropiado (por ejemplo: bóveda de contraseñas).
e) La selección de contraseñas en función de:

- Selección de contraseñas de una longitud mínima no menor a los 8 caracteres.
- Ser fáciles de recordar.
- No incluyan caracteres consecutivos idénticos.

ISO 27.001 A.9.3.1 [1] – ISO 27.002 9.3.1 [14]

RH2.1.5	Nivel C	F

Macroproceso de formación

La organización deberá capacitar a los usuarios (propios, contratistas y de terceras partes) sobre:

a) La selección de contraseñas en función de:

- Selección de contraseñas de una longitud mínima no menor a los 10 caracteres.
- No incluyan todos caracteres numéricos o alfabéticos.
- No ser vulnerables a ataques de diccionario (no contener palabras utilizadas en diccionarios).
- No estén basadas en algo que otra persona pueda adivinar u obtener fácilmente utilizando información relacionada con la persona, por ejemplo: nombres, números telefónicos y fechas de nacimiento, etc.

b) Si la información secreta de autenticación es provisoria, cambiarlas inmediatamente al iniciar sesión.

a) y b) deben ser requeridos obligatoriamente por sistema.

La organización no deberá almacenar información de autenticación secreta en formato plano o cifrado, únicamente se deberá almacenar su hash (utilizando algoritmos de hashing públicamente probados y reconocidos por la comunidad como seguros en el mediano plazo) cifrado. Para el caso de las claves criptográficas, las mismas se deberán almacenar a través de algún mecanismo de cifrado o en formato físico. Se deberá asegurar la protección apropiada de las contraseñas cuando éstas se utilizan como información secreta de autenticación en procesos automáticos de inicio de sesión y se encuentren almacenadas.
ISO 27.002 9.3.1 [14]

RH2.1.6	Nivel C	F
Macroproceso de formación		
Se deberá establecer un Programa de Conciencia, Entrenamiento y Difusión de la SI. El programa de concientización de SI deberá tener como objetivo concientizar a los empleados y, cuando sea pertinente, a los contratistas, sobre sus responsabilidades con respecto a la SI y la forma mediante la cual se cumple con dichas responsabilidades.		
ISO 27.002 7.2.2 [14]		

RH2.1.7	Nivel C	F
Macroproceso de formación		
El programa de Conciencia, Entrenamiento y Difusión en SI de acuerdo con las políticas de SI de la organización y los procesos pertinentes, teniendo en cuenta la información de la organización a proteger y los controles que se han implementado para proteger la información. El programa de Conciencia, Entrenamiento y Difusión incluirá varias actividades diversas destinadas a elevar el nivel de concientización del personal propio, contratistas y de terceros.		

Se deberá planificar el programa de Conciencia, Entrenamiento y Difusión teniendo en cuenta los roles de los empleados en la organización y, cuando corresponda, las expectativas de la organización con respecto a la concientización de los contratistas. Las actividades del programa se programarán a lo largo del tiempo, de manera regular, para que las actividades se repitan en el tiempo e incorporen a nuevos empleados y contratistas. A su vez, el programa se actualizará regularmente para mantenerse alineado con las políticas y los procedimientos de la organización, y que se nutra de las lecciones aprendidas a partir de los incidentes de SI.

ISO 27.002 7.2.2 [14]

RH2.1.8	Nivel C	F

Macroproceso de formación

La formación en SI deberá cubrir aspectos generales como:

a) La declaración del compromiso de la dirección para con la SI a lo largo de toda la organización.
b) La necesidad de familiarizarse y cumplir con las reglas y obligaciones aplicables de SI, tal como se las define en las políticas, normas, leyes, regulaciones, contratos y acuerdos.
c) La responsabilidad personal y obligación de rendir cuentas por sus propias acciones u omisiones, y las responsabilidades generales relacionadas con la protección y la SI que pertenece a la organización y a las terceras partes;
d) Los procedimientos básicos de SI (por ejemplo, los reportes de incidentes de SI) y los controles básicos (por ejemplo, seguridad de las contraseñas, controles contra código malicioso y escritorios limpios).
e) Los puntos de contacto y los recursos para obtener información o asesoramiento adicional sobre asuntos de SI incluyendo material adicional para la educación y la capacitación en SI.

La educación y la capacitación en SI se deberán realizar periódicamente. La educación y la capacitación iniciales aplican a quienes sean transferidos a nuevos cargos o roles con requisitos de SI significativamente distintos, no solo a personas nuevas, y se recomienda realizarlas antes de que se active el nuevo rol.

El programa deberá encontrarse alineado con las políticas de SI y los procedimientos pertinentes de la organización, teniendo en cuenta la información de la organización a proteger y los controles que se han implementado para proteger esta información. El programa deberá considerar distintas formas de educación y capacitación.
ISO 27.002 7.2.2 [14]

RH2.1.7	Nivel B	F
Macroproceso de formación		
La organización deberá capacitar a los usuarios (propios, contratistas y de terceras partes) sobre: a) La selección de contraseñas en función de: ▪ Selección de contraseñas de una longitud mínima no menor a los 16 caracteres. ▪ Una técnica que permita el fácil recuerdo de las mismas (utilizando canciones, proverbios o frases de común conocimiento). b) La prohibición de acceder a los sistemas o servicios de la organización a través de redes públicas sin utilizar una red privada virtual. No se deberá permitir el blanqueo de contraseñas únicamente a partir del mecanismo de preguntas secretas. Deberá de establecerse un mecanismo de al menos 3 desafíos (por ejemplo: pregunta secreta, código de token y autenticación vía teléfono).		
ISO 27.002 9.3.1 [14]		

RH2.1.8	Nivel A	F
Macroproceso de formación		
La organización deberá implementar sistemas de autenticación única (“*SSO*”, por sus siglas en inglés) u otras herramientas similares de gestión de información secreta de autenticación.		

Debido a que se tendrá un único punto de falla (única contraseña), la misma deberá cumplir con todos los requisitos del presente Dominio de Seguridad y además deberá:

a) No tener una longitud mínima menos a los 22 caracteres.
b) Poseer al menos 3 caracteres especiales, 3 caracteres en minúscula, 3 caracteres en mayúscula y 3 caracteres numéricos.

La organización deberá estar atenta a posibles nuevos mecanismos que reemplacen el actual uso del mecanismo de autenticación secreta.

ISO 27.002 9.3.1 [14]

RH2.1.9	Nivel A	F

Macroproceso de formación

La organización deberá implementar un sistema de fidelización dentro del programa de Conciencia, Entrenamiento y Difusión en SI, dentro del cual el personal de la organización podrá ser acreedor de una gran variedad de premios al completar diversas actividades del programa de Conciencia, Entrenamiento y Difusión.

A su vez, se deberán establecer caminos a seguir durante la inducción, cambios de roles, implementación de cambios, licencias, suspensiones, despidos o terminaciones de contratos como parte del sistema de fidelización, recompensando monetariamente o con premios a quienes cumplan con cada etapa del camino a seguir.

Cada RRHH de la organización coleccionará puntos de seguridad por cada acción del camino a seguir o actividad del programa de Conciencia, Entrenamiento y Difusión que desarrolle en forma completa y exitosa. Los puntos de seguridad podrán ser canjeados por premios.

ISO 27.002 9.3.1 [14]

[Página dejada en blanco intencionalmente]

GESTIÓN DE LA CONTINUIDAD

El objetivo primordial del presente subsistema consiste en establecer los lineamientos para la continuidad de la Seguridad de la Información. Requerido principalmente dentro de los niveles C y B del Modelo de Madurez del MRU, dichos lineamientos conforman uno de los principios para alcanzar la mejora continua en Seguridad de la Información.

GC1 Continuidad de la Seguridad de la Información

GC1.1 Lineamientos & Sistema de continuidad

GC1 CONTINUIDAD DE LA SEGURIDAD

GC1.1 Lineamientos & Sistema de Continuidad

Objetivo Establecer los fundamentos de nivel "C" de la continuidad de la Seguridad de la Información, como primer acercamiento hacia la continuidad en materia de seguridad. Los niveles de madurez superiores establecerán todos los lineamientos necesarios para alcanzar la mejora continua en continuidad de la Seguridad de la Información.

GC1.1.1	Nivel C	F
Macroproceso de continuidad de la seguridad		
La organización debe determinar sus requisitos de SI y de la continuidad de la gestión de la SI en situaciones adversas, por ejemplo, durante una crisis o un desastre. *Se recomienda que la organización determine si la continuidad de la SI está incluida dentro del proceso de gestión de la continuidad del negocio o dentro del proceso de gestión de la recuperación ante desastres.* Se deberán determinar los requisitos de SI al planificar la continuidad del negocio y la recuperación ante desastres.		

En la ausencia de una planificación formal de continuidad del negocio y de recuperación ante desastres, se recomienda que la gestión de la SI asuma que los requisitos de SI permanecen iguales en situaciones adversas, comparados con los de las condiciones normales de operación. Alternativamente, una organización puede realizar un análisis de impacto al negocio para los aspectos de SI con el fin de determinar los requisitos de SI aplicables en situaciones adversas.

Con el fin de reducir el tiempo y el esfuerzo de un análisis de impacto al negocio, se deberá incluir los aspectos de SI dentro del análisis de impacto al negocio de la gestión de continuidad o de la gestión de la recuperación ante desastres. Por lo tanto, los requisitos de continuidad de la SI estarán explícitamente formulados en los procesos de gestión de la continuidad del negocio y de gestión de la recuperación ante desastres.

ISO 27.001 A.17.1.1 [1] – ISO 27.002 17.1.1 [14]

GC1.1.2	Nivel	F

Macroproceso de continuidad de la seguridad

La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la SI durante una situación adversa.

Por lo tanto, deberá garantizar que:

a) Exista una estructura de gestión adecuada a fin de prepararse, mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencia necesarias.
b) Se designe al personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para gestionar un incidente y mantener la SI.
c) Se desarrollen y aprueben planes documentados, procedimientos de respuesta y recuperación, detallando la manera en que la organización gestionará un evento disruptivo y mantendrá la seguridad de su información en un nivel predeterminado, basado en los objetivos de continuidad de la SI aprobados por la dirección.

ISO 27.001 A.17.1.2 [1] – ISO 27.002 17.1.2 [14]

GC1.1.3	Nivel	F
Macroproceso de continuidad de la seguridad		
La organización debe verificar a intervalos regulares, los controles de la continuidad de la SI, establecidos e implementados, para asegurar que sean válidos y eficaces durante situaciones adversas. Los cambios a la organización, técnicos, a los procedimientos y a los procesos, ya sea en el contexto operativo o de continuidad, pueden producir cambios en los requisitos de continuidad de la SI. En tales casos, se deberá revisar la continuidad de los procesos, los procedimientos y los controles de SI con respecto a estos cambios en los requisitos.		
ISO 27.001 A.17.1.3 [1] – ISO 27.002 17.1.3 [14]		

GC1.1.4	Nivel	F
Macroproceso de continuidad de la seguridad		
La organización deberá implementar las instalaciones de procesamiento de la información con redundancia suficiente para cumplir con los requisitos de disponibilidad. A su vez, deberá identificar los requisitos de negocio para la disponibilidad de los sistemas de información. Cuando no se puede garantizar la disponibilidad utilizando la arquitectura existente de los sistemas, se deben considerar componentes o arquitecturas redundantes. Cuando corresponda, se deberán probar los sistemas de información redundantes para garantizar que la transición de un componente a otro en caso de falla funcione de la manera esperada. *La implementación de redundancias puede introducir riesgos a la integridad o la confidencialidad de la información y de los sistemas de información, los cuales necesitan considerarse al diseñar los sistemas de información.*		
ISO 27.001 A.17.2.1 [1] – ISO 27.002 17.2.1 [14]		

GC1.1.5	Nivel	F
Macroproceso de continuidad de la seguridad		
En función de los requisitos de continuidad de la SI, la organización deberá establecer, documentar, implementar y mantener: a) Los controles de SI dentro de los procesos y los procedimientos de continuidad del negocio o recuperación ante desastres, y de sus sistemas y herramientas de apoyo. b) Los procesos, los procedimientos y los cambios para la implementación a fin de mantener los controles de SI existentes durante una situación adversa. c) Los controles compensatorios para aquellos controles de SI que no se puedan mantener durante una situación adversa. En el contexto de la continuidad del negocio o de la recuperación ante desastres, se pueden haber definido procesos o procedimientos específicos. Se deberá proteger la información que se maneja dentro de estos procesos y procedimientos o dentro de los sistemas de información dedicados que los apoyan. Por lo tanto, la organización involucrará a los especialistas en SI cuando se establecen, implementan y mantienen los procesos y procedimientos de continuidad de negocio o recuperación ante desastres. Los controles de SI que ya se hayan implementado deberán continuar operando durante una situación adversa. Si dichos controles no pueden seguir asegurando la información, se recomienda establecer, implementar y mantener otros controles para mantener un nivel aceptable de SI.		
ISO 27.001 A.17.2.1 [1] – ISO 27.002 17.2.1 [14]		

GC1.1.6	Nivel	F
Macroproceso de continuidad de la seguridad		
La organización deberá verificar la continuidad de la gestión de la SI a través de: a) Ejercicios y pruebas a la funcionalidad de los procesos, procedimientos y controles de continuidad de la SI para garantizar que sean coherentes con los objetivos de continuidad de la SI.		

b) Ejercicios y pruebas del conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la SI a fin de garantizar que su desempeño sea coherente con los objetivos de continuidad de la SI.
c) Revisión de la validez y la eficacia de las medidas de continuidad de la SI cuando ocurren cambios en los sistemas de información, en los procesos, procedimientos y controles de SI, o en los procesos y soluciones para la gestión de la continuidad del negocio o la recuperación ante desastres.

La verificación de los controles de la continuidad de la SI es diferente de las pruebas y la verificación de la SI en general, por lo que deberá realizarse por fuera de las pruebas de los cambios. En lo posible, es preferible integrar la verificación de los controles de continuidad de la SI con las pruebas de continuidad de negocio o recuperación ante desastres de la organización.

ISO 27.001 A.17.1.3 [1] – ISO 27.002 17.1.3 [14]

GC1.1.7	Nivel	F

Macroproceso de continuidad de la seguridad

La organización deberá diseñar, implementar y mantener un Sistema de Continuidad de la SI, el cual deberá contener al menos los siguientes componentes:

a) Política de continuidad de la SI.
b) Responsabilidades y roles definidos vinculados a la continuidad de la SI.
c) Procesos de gestión de:
- Políticas.
- Planeamiento.
- Implementación y operación.
- Revisión gerencial.
- Mejora continua.
- Monitoreo y performance.

d) Cualquier proceso de continuidad relevante para la organización.
e) Alcance del sistema (compatible a lo establecido en LS1.1.4).

ISO 22.301 0.1 y 4.1 [27]

GC1.1.8	Nivel	F
Macroproceso de continuidad de la seguridad		
El diseño del Sistema de Continuidad de la SI deberá tener en cuenta el contexto de la organización definido en (LS1.1.1, LS1.1.2 y LS1.1.3) y, a su vez, los siguientes componentes vinculados o complementarios al mismo: a) Las actividades, funciones, procesos, servicios, productos y relaciones de la organización. b) La cadena de valor de la organización. c) El apetito de riesgo de la organización (GR1.1.4). d) Vínculos y relación entre la política de continuidad del negocio y la política de continuidad de la SI. Todos estos elementos serán considerados durante el diseño del Sistema de Continuidad de la SI configurando el contexto de este, en conjunto con los siguientes elementos: a) Objetivos de continuidad del negocio y de continuidad de la SI. b) Propósito del Sistema de Continuidad de la SI. c) Las partes interesadas relevantes al Sistema de Continuidad de la SI. d) Los requerimientos de estas partes interesadas detalladas en c). e) Requerimientos legales, regulatorios, estatutarios, contractuales y de mercado.		
ISO 22.301 4.1, 4.2.1 y 4.2.2 [27]		

GC1.1.9	Nivel	F
Macroproceso de continuidad de la seguridad		
La organización deberá: a) Establecer las partes/sectores de la organización que serán incluidas dentro del Sistema de Continuidad de la SI. b) Establecer los requerimientos del Sistema de Continuidad de la SI (en función de los objetivos, misión, requerimientos y obligaciones de la organización). c) Identificar los productos y servicios de la organización vinculados con el alcance del Sistema de Continuidad de la SI.		

d) Tomar en consideración todas las partes interesadas vinculadas a la continuidad de la seguridad.
ISO 22.301 4.3.2 [27]

GC1.1.10	Nivel	F
Macroproceso de continuidad de la seguridad		
La dirección ejecutiva y el órgano rector de gobierno de la organización deberán demostrar y documentar su compromiso con el diseño, establecimiento, mejora y ejecución del Sistema de Continuidad de la SI. La política de Continuidad de la SI deberá ser firmada y avalada por la dirección ejecutiva y el órgano rector de gobierno. La dirección ejecutiva y el órgano rector de gobierno de la organización deberán apoyar la mejora continua del Sistema de Continuidad de la SI.		
ISO 22.301 5.2 y 5.3 [27]		

GC1.1.11	Nivel	F
Macroproceso de continuidad de la seguridad		
La política de Continuidad de la SI deberá: a) Encontrarse disponible y adecuadamente documentada. b) Ser comunicada a toda la organización y partes interesadas relevantes. c) Encontrarse disponible para las partes interesadas relevantes. d) Ser revisada y mejorada continuamente.		
ISO 22.301 5.2 y 5.3 [27]		

[Página dejada en blanco intencionalmente]

SEGUIMIENTO Y CONTROL

El objetivo primordial del presente subsistema comprende tanto la revisión gerencial del Sistema de Mejora Continua en Seguridad de la Información de la organización como la realización de auditorías sobre el mismo. A su vez, se establecerán los lineamientos fundamentales sobre la evaluación de las actividades, proyectos y procesos de seguridad de la organización a través del empleo de métricas y su monitoreo periódico. Por otro lado, se sentarán las bases para las realizaciones de auditorías periódicas y la gestión de sus resultados y las no conformidades que hayan sido identificadas.

SC1 Revisión gerencial de la Seguridad de la Información

SC1.1 Evaluación y Monitoreo de la Seguridad de la Información

SC1.2 No conformidades y acciones correctivas

SC2 Auditoria de la Seguridad de la Información

SC2.1 Lineamientos de Auditoria de Seguridad de la Información

SC1 REVISIÓN GERENCIAL DE LA SEGURIDAD

SC1.1 Evaluación y monitoreo de la SI

Objetivo Establecer los fundamentos de la revisión gerencial del Sistema de Mejora Continua en Seguridad de la Información de la organización.

SC1.1.1	Nivel E	F
Proceso de evaluación de la seguridad		
La organización deberá evaluar periódicamente el desempeño y la efectividad de las actividades de gestión de los Activos de Información de la organización. Para la implementación del presente requerimiento, la organización deberá como mínimo determinar: a) Si el relevamiento de Activos de Información se ha realizado conforme al alcance establecido por la organización según LS1.1.4. b) Si se ha asignado un responsable a todos los Activos de Información de la organización. c) Si se han clasificado todos los Activos de Información de la organización en función de LS2.3.6. d) El cumplimiento con el requerimiento LS2.3.4 relativo a la documentación y mantenimiento del inventario de Activos de información de la organización.		
LS1.1.4 – LS2.3.4 - LS2.3.6		

SC 1.1.2	Nivel D	F
Proceso de evaluación de la seguridad		
La organización deberá evaluar periódicamente el desempeño y la efectividad de las actividades de gestión de riesgos de SI. Para la implementación del presente requerimiento, la organización deberá determinar: a) La correcta revisión de la gestión de riesgos de SI y del apetito de riesgo de la organización. b) La efectividad de las acciones de tratamiento de riesgos de SI. c) La efectividad de la evaluación y tratamiento de riesgos de SI. d) La correcta definición de roles y autoridades de gestión de riesgos de SI (en función de lo definido en el Subsistema GR).		
GR		

SC 1.1.3	Nivel D	F
Proceso de evaluación de la seguridad		
Los resultados de la evaluación del desempeño, seguimiento y las mediciones vinculadas a la SI realizadas por la organización deberán documentarse y conservarse para permitir la comparación del progreso de estas a lo largo del tiempo.		
ISO 27.001 9.1 [1] - ISO 27.004 0.1 [15]		

SC 1.1.4	Nivel D	F
Proceso de evaluación de la seguridad		
La dirección ejecutiva debe revisar periódicamente que los procesamientos y los procedimientos de la información dentro de su área de responsabilidad cumplan con las políticas, los procesos y cualquier otro tipo de lineamiento de seguridad requerido por el Sistema de Mejora Continua en SI.		

Si se encuentra cualquier incumplimiento como resultado de la revisión, se recomienda que los gerentes:

a) Determinen las causas del incumplimiento.
b) Evalúen la necesidad de realizar acciones para lograr el cumplimiento.
c) Implementen las acciones correctivas apropiadas.
d) Revisen las acciones correctivas realizadas para verificar su eficacia e identificar cualquier deficiencia o vulnerabilidad.

Se deberá registrar los resultados de las revisiones y las acciones correctivas realizadas por los gerentes, y se deberá mantener estos registros. Cuando se realice una revisión independiente dentro de su área de responsabilidad, los gerentes informen estos resultados a las personas que realizan dicha revisión.

ISO 27.001 A.18.2.2 [1] – ISO 27.002 18.2.2 [14]

SC 1.1.5	Nivel C	F

Proceso de evaluación de la seguridad

La organización deberá evaluar periódicamente el desempeño de las actividades de SI y la eficacia del Sistema de Mejora Continua de SI.

Para la implementación del presente requerimiento, la organización deberá determinar:

a) Que se necesita seguir y medir, incluyendo los procesos y los controles de SI.
b) Los métodos para realizar el seguimiento, medición, análisis y los controles de SI.
c) Cuando se debe realizar el seguimiento y la medición.
d) Quien debe realizar el seguimiento y la medición.
e) Cuando se deben analizar y evaluar los resultados del seguimiento y de la medición.
f) Quien debe analizar y evaluar estos resultados.

ISO 27.001 9.1 [1]

SC 1.1.6	Nivel C	F
Proceso de evaluación de la seguridad		
Se deberá revisar el enfoque de la organización para la gestión de la SI y su implementación (objetivos de control, controles, políticas, procesos y procedimientos para la SI), en forma independiente a intervalos planificados o cuando ocurran cambios significativos. Aquellas situaciones que califican como cambios significativos se encuentran detalladas en GR1.1.4. Se recomienda que la dirección inicie la revisión independiente. Esta revisión independiente es necesaria para garantizar que el enfoque de la organización para gestionar la SI continúe siendo correcto, adecuado y eficaz. La revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque con respecto a la seguridad, incluyendo la política y los objetivos de control. Esta revisión deberá ser realizada por personas independientes del área bajo revisión. Las personas que realicen estas revisiones deberán poseer las habilidades y la experiencia adecuadas. Los resultados de la revisión independiente se registrarán e informaran a la dirección que inició la revisión. La organización deberá mantener estos registros. Si la revisión independiente identifica que el enfoque de la organización para la gestión de la SI y la implementación no son adecuados, la dirección deberá considerar acciones correctivas.		
ISO 27.001 A.18.2.1 [1] – ISO 27.002 18.2.1 [14]		

SC 1.1.7	Nivel C	F
Proceso de evaluación de la seguridad		
La organización deberá revisar periódicamente los sistemas de información para verificar que cumplan con las políticas y las normas de SI de la organización.		

Se debe revisar el cumplimiento técnico preferentemente con la asistencia de herramientas automáticas. Se deben a su vez, utilizar pruebas de penetración o de evaluación de las vulnerabilidades. Dichas pruebas deben ser planificadas, documentadas y repetibles. Cualquier revisión de cumplimiento técnico deberá ser realizada solo por personas competentes y autorizadas, o bajo la supervisión de tales personas.
ISO 27.001 A.18.2.3 [1] – ISO 27.002 18.2.3 [14]

SC 1.1.8	Nivel B	F
Proceso de evaluación de la seguridad		
La organización deberá evaluar periódicamente a su vez, la eficiencia del Sistema de Mejora Continua de SI y la efectividad de: a) Las actividades, procedimientos, procesos y Macroprocesos de SI. b) El programa de Toma de Conciencia, Entrenamiento y Difusión del MRU. c) El programa de Programa de Evaluación y Monitoreo de SI. d) Los controles, grupos de controles y lineamientos del estadio de madurez objetivo de la organización. e) La PSI y todas las políticas de SI de la organización. *d) incluye a su vez todos los requerimientos de los estadios de madurez inferiores al nivel seleccionado por la organización.*		
ISO 27.004 0.1 [15]		

SC 1.1.9	Nivel B	F
Proceso de evaluación de la seguridad		
La organización deberá establecer un Programa de Evaluación y Monitoreo de SI.		

El Programa de Evaluación y Monitoreo de SI conforma el llamado "Programa de Medición de SI" definido por la ISO 27.004 0.1 [15].

Dicho programa deberá:

a) Respaldar el proceso de evaluación y monitoreo de SI.
b) Colaborar en la determinación de la necesidad o no de modificación o mejora de los procesos, actividades, controles, procedimientos o políticas de SI.
c) Asistir a la dirección ejecutiva en la identificación y evaluación de los no cumplimientos e ineficacias de los procesos, actividades, controles, procedimientos o políticas de SI.
d) Asistir en la priorización de las necesidades de mejora o modificación determinadas en b).
e) Definir cómo medir la efectividad de los procesos, actividades, controles, procedimientos o políticas de SI.
f) Definir como las mediciones detalladas en e) serán utilizadas para evaluar la efectividad de los procesos, actividades, controles, procedimientos o políticas de SI para producir resultados comparables y reproducibles.
f) Medir la efectividad de los procesos, actividades, controles, procedimientos o políticas de SI.
g) Establecer el proceso de Evaluación y Monitoreo de SI (detallado en SC1.1.7).

El alcance del programa deberá abarcar a toda la organización en su conjunto, incluyendo los puntos de contacto con las partes interesadas externas.

Debe recordarse que ninguna medición brindara la completa seguridad de la ejecución de controles o de la suficiencia o efectividad de estos. La presente actividad constituye una herramienta adicional del CISO de la organización para realizar el seguimiento y control de las actividades de SI y del Sistema de Mejora Continua de SI de la organización.

ISO 27.001 9.1 [1] - ISO 27.004 0.1 y 0.2 [15]

SC 1.1.10	Nivel B	F
Proceso de evaluación de la seguridad		
La organización deberá establecer un proceso de Evaluación y Monitoreo de SI en el marco del Programa detallado en SC1.1.6.		

Dicho proceso contará con los siguientes subprocesos: a) Desarrollo de mediciones (mediciones base, derivadas e indicadores). b) Implementación y operación de la Evaluación y Monitoreo de la SI. c) Recolección y análisis de datos. d) Preparación de los resultados de las mediciones. e) Comunicación de los resultados de las mediciones desarrolladas a las partes interesadas. f) Identificación de necesidades de mejora del Sistema de Mejora Continua de SI de la organización, incluyendo su alcance, políticas, objetivos, controles, procesos, actividades y procedimientos de SI. g) Mejora continua del Programa de Evaluación y Monitoreo de SI.
ISO 27.004 0.2 [15]

SC 1.1.11	Nivel B	F
Proceso de evaluación de la seguridad		
Se deberán utilizar herramientas automáticas de medición y de reporte.		
ISO 27.002 18.2.2 [14]		

SC1 EVALUACIÓN GERENCIAL DE LA SEGURIDAD

SC1.2 No conformidades y acciones correctivas

Objetivo Establecer los fundamentos de la identificación y tratamiento de las no conformidades y, a su vez, de las acciones correctivas que la organización deberá diseñar, implementar y mantener para lidiar con estas no conformidades.

SC1.2.1	Nivel D	F
Macroproceso de revisión gerencial		
La organización deberá realizar una revisión gerencial de su Sistema de Mejora Continua de SI, con el objetivo de identificar y documentar no conformidades. Una no conformidad configura cualquier incumplimiento de los requerimientos establecidos por el MRU vinculados al estadio de madurez objetivo de la organización y todos los estadios inferiores al mismo.		

SC1.2.2	Nivel D	F
Macroproceso de revisión gerencial		
La organización deberá tomar acciones correctivas para todas aquellas no conformidades vinculadas a los subsistemas de Gestión de riesgos y Lineamientos de Seguridad. Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.		

SC1.2.3	Nivel D	F
Macroproceso de revisión gerencial		
La organización deberá conservar información documentada como evidencia de: a) La realización de la revisión gerencial y la búsqueda de no conformidades establecida en PM2.1.1. b) La naturaleza de las no conformidades y todas las acciones realizadas posteriormente. c) Los resultados de todas las acciones correctivas.		

SC1.2.4	Nivel D	F
Macroproceso de revisión gerencial		
Cuando ocurra una no conformidad, la organización deberá: a) Reaccionar ante la misma si se encuentra vinculada a los subsistemas de Gestión de riesgos y Lineamientos de Seguridad. b) Documentar la no conformidad. c) Evaluar la necesidad de acciones para eliminar sus causas.		

d) Planificar e implementar los cambios al Sistema de Mejora Continua de SI de la Organización que considere necesarios. Los cambios establecidos en d) deberán documentarse y mantenerse en el tiempo.
ISO 27.001 10.1 [1]

SC1.2.5	Nivel C	F
Macroproceso de revisión gerencial		
Cuando ocurra una no conformidad, la organización deberá: a) Reaccionar ante la misma a través de la implementación de todas las acciones que considere necesarias para controlarla y corregirla. b) Actuar sobre sus consecuencias. c) Evaluar la necesidad de acciones para eliminar sus causas a través de: *I. La revisión de la no conformidad.* *II. La determinación de las causas de la no conformidad.* *III. La determinación de la existencia de no conformidades similares, o su potencial existencia.* d) Implementar las acciones que a través de c) considere necesarias. e) Revisar la eficiencia de todas las acciones correctivas realizadas. f) Planificar e implementar los cambios al Sistema de Mejora Continua de SI de la Organización que considere necesarios. Los cambios establecidos en f) deberán documentarse y mantenerse en el tiempo. La organización deberá tomar acciones correctivas para todas aquellas no conformidades vinculadas a los estadios de madurez “E”, “D” y “C”.		
ISO 27.001 10.1 [1]		

SC1.2.6	Nivel C	F
Macroproceso de revisión gerencial		
El CIPO de la organización deberá: a) Realizar revisiones gerenciales periódicas sobre el Sistema de Mejora Continua en SI con el objetivo de identificar no conformidades y posibles puntos de mejora. b) Diseñar los planes de mejora y solución de conformidades. c) Gestionar el cambio. d) Gestionar la formación y capacitación global en SI. e) Implementar y supervisar las mejoras diseñadas en b) en conjunto con los responsables de negocio y seguridad correspondientes.		

SC1.2.6	Nivel C	F
Macroproceso de revisión gerencial		
La organización deberá diseñar, implementar y mantener una política de gestión de vulnerabilidades (tanto técnicas como no técnicas). Dicha política fijara los lineamientos y los procesos a seguir para identificar, registrar, tratar y monitorear las vulnerabilidades de seguridad de la organización.		

SC1.2.7	Nivel B	F
Macroproceso de revisión gerencial		
La organización deberá tomar acciones correctivas para todas aquellas no conformidades vinculadas a los estadios de madurez “E”, “D”, “C” y “B”.		

SC1.2.8	Nivel A	F
Macroproceso de revisión gerencial		
La organización deberá tomar acciones correctivas para todas las no conformidades que han sido identificadas.		

SC2 AUDITORIA DE LA SEGURIDAD

SC2.1 Lineamientos de Auditoria de SI

Objetivo Establecer los fundamentos de la Auditoria de Seguridad que deberá llevar adelante la organización. Dichos lineamientos gobernarán tanto el diseño de los programas como la ejecución de las actividades de auditoria de seguridad tanto interna como independiente.

SC2.1.1	Nivel C	F
Macroproceso de auditoria de la seguridad		
La organización deberá realizar auditorías internas a intervalos planificados para proporcionar información acerca de si el Sistema de Mejora Continua de la organización: a) Es conforme con: I. *Los requisitos de la propia organización para su Sistema de Mejora Continua.* II. *Los requisitos y lineamientos del MRU relativos al estadio de madurez objetivo de la organización.* III. *Los requisitos legales, regulatorios, estatutarios, contractuales y de mercado.* b) Se implementa, mantiene y mejora eficazmente.		
ISO 27.001 9.2.a y 9.2.b [1]		

SC2.1.2	Nivel C	F
Macroproceso de auditoria de la seguridad		
La organización deberá planificar, establecer, implementar y mantener uno o más programas de auditoria de SI. Los programas de auditoria de SI deberán incluir: a) La frecuencia. b) Los métodos a utilizar. c) Las responsabilidades. d) Los requisitos de planificación. e) Los requisitos de presentación de informes. Los programas de auditoria de SI deberán tomar en cuenta la criticidad de los procesos de negocio involucrados, la gestión de riesgos de SI y los resultados de auditorías previas. *Durante la implementación de c) debe recordarse que el RASI es el responsable máximo por el diseño, planificación, implementación y mejora de los programas de auditoria de SI. No obstante, el RASI podrá delegar cualquiera de las tareas a sus subordinados u otras autoridades de SI por las cuales continuará siendo responsable.*		
ISO 27.001 9.2.c [1]		

SC2.1.3	Nivel C	F
Macroproceso de auditoria de la seguridad		
El CSI deberá: a) Definir las prioridades de auditoria de SI y proponer el alcance de cada auditoria de SI al RASI. b) Poder ordenar el inicio de las actividades de auditoria de seguridad, pero no podrá detenerlas o suspenderlas.		
ISO 27.001 9.2 [1]		

SC2.1.4	Nivel C	F
Macroproceso de auditoria de la seguridad		
El RASI deberá: a) Diseñar, planificar, establecer, implementar y mantener los programas de auditoria de SI. b) Seleccionar auditores y realizar auditorías de SI que aseguren la objetividad y la imparcialidad del proceso de auditoría. c) Asegurar que los resultados de las auditorias de SI se informen a las partes interesadas pertinentes, al CSI y al CISO de la organización. d) Conservar información documentada como evidencia de los programas de auditoria de SI y los resultados de auditoria. e) Definir los criterios de auditoria de SI y el alcance de cada auditoria de SI. f) Registrar y documentar todas sus actividades.		
ISO 27.001 9.2 [1]		

SC2.1.5	Nivel C	F
Macroproceso de auditoria de la seguridad		
El RASI de la organización deberá contar con total libertad para realizar auditorías aleatorias y sorpresivas de SI sobre cualquier área, proceso, actividad, control, activo de información o recurso de la organización. La libertad de acceso del RASI deberá basarse exclusivamente en la búsqueda de no conformidades e identificación de oportunidades de mejora del Sistema de Mejora Continua de la organización. *Se respetará la independencia del área de auditoría, por lo que el CISO y el CEO tendrán la autoridad de requerir al área de auditoría el inicio de cierta actividad/proceso vinculado a su tarea. No obstante, el área de auditoría no tendrá obligación alguna de suspender o finalizar sus actividades/procesos a requerimiento del CISO, CEO o CSI.*		
LS2.1.5		
ISO 27.001 9.2 [1] – LS2.1.5 [2]		

SC2.1.6	Nivel C	F
Macroproceso de auditoria de la seguridad		
A fin de minimizar las interrupciones de los procesos de negocio, se debe planificar cuidadosamente y acordar los requisitos y las actividades de auditoría que involucren la verificación de los sistemas en producción. Para lo cual se deberán considerar los lineamientos siguientes: a) Que los requisitos de auditoría para el acceso a los sistemas y los datos se acuerden con la gerencia que corresponda. b) Que se acuerde y controle el alcance de las pruebas de auditoría técnica; c) Que las pruebas de auditoría se encuentren limitadas a un acceso de sólo lectura en lo referente al software y a los datos. d) Que cualquier acceso que no sea de sólo lectura solamente se permita a copias aisladas de archivos del sistema, las cuales se recomienda eliminar una vez finalizada la auditoría, o se les otorgue protección apropiada si existe una obligación de mantener dichos archivos como requisito de documentación de la auditoría. e) Que se identifiquen y acuerden los requisitos para efectuar procesamiento especial o adicional. f) Que las pruebas de auditoría que puedan afectar a la disponibilidad del sistema se realicen fuera del horario laboral. g) Que se monitoreen y registren todos los accesos para generar un rastro de referencia.		
ISO 27.001 A.12.7.1 [1] – ISO 27.002 12.7.1		

[Página dejada en blanco intencionalmente]

PROCESOS Y MEJORA CONTINUA

El objetivo primordial del presente subsistema comprende el establecimiento de los lineamientos de la gestión por procesos de la Seguridad de la Información. Este enfoque orientado a la calidad y efectividad de las actividades de seguridad, mejorará significativamente la gestión del cambio, la documentación, la implementación y la adaptabilidad a cambios de los lineamientos y controles de Seguridad de la Información de la organización.

A su vez, se enfoca en el diseño y establecimiento del programa de mejora continua en Seguridad de la Información, pieza clave del Modelo de Madurez del MRU.

PM1 Procesos de Seguridad de la Información

PM1.1 Lineamientos de la gestión de SI orientada a procesos

PM2 Mejora Continua de la Seguridad de la Información

PM2.1 Programa de mejora continua & compliance de SI

PM1 Procesos de SI

PM1.1 Lineamientos de la gestión de SI orientada a procesos

Objetivo Establecer los fundamentos de la Seguridad de la Información basada en procesos, para así facilitar tanto la gestión del cambio como el tiempo de respuesta de la organización ante mejoras y necesidades de adaptación a amenazas, lineamientos y requerimientos de seguridad.

PM1.1.1	Nivel D	F
Macroproceso de gestión de procesos		
La organización deberá diseñar los procesos de negocio de la organización vinculados a la SI.		

PM1.1.2	Nivel C	F
Macroproceso de gestión de procesos		
La organización deberá diseñar, modelar, implementar, mejorar y documentar los procesos de negocio de la organización vinculados a la SI. Deberá a su vez, realizar formaciones y capacitaciones periódicas para todos los actores vinculados a los procesos y para las partes interesadas correspondientes. *La documentación de los procesos deberá encontrarse basada en los lineamientos establecidos por el MRU (documentación de alto y bajo nivel).*		

PM1.1.3	Nivel C	F
Macroproceso de gestión de procesos		
La organización deberá diseñar y mantener constantemente actualizado un mapa de macroprocesos de SI.		

PM1.1.4	Nivel B	F
Macroproceso de gestión de procesos		
La organización deberá contar con un área de gestión de procesos de negocio. Las actividades de dicha área deberán alcanzar al menos a todos los procesos de negocio de la organización vinculados a la SI. El área de gestión de procesos de negocio deberá: a) Formar parte de la dirección ejecutiva.		

b) Ser el responsable global del diseño, modelado, implementación, ejecución, mejora y documentación de los procesos de negocio bajo su alcance. Deberá trabajar en conjunto con los responsables funcionales y de negocio
c) Ser establecida por la dirección ejecutiva y poseer su compromiso en cuanto a recursos y potestad para relevar todas las áreas, procesos, procedimientos y actividades de la organización bajo su alcance.
d) Poseer un alcance de acción establecido por la dirección ejecutiva de la organización.
e) Mejorar continuamente los procesos de la organización bajo su alcance.
f) Realizar revisiones gerenciales periódicas sobre los procesos de la organización bajo su alcance.
g) Capacitar a los responsables de procesos y a todos los actores involucrados en cada uno de los procesos sobre la realización de sus actividades y el seguimiento de los procesos a los cuales están vinculados.
h) Nombrar a los responsables de procesos.

El área de gestión de procesos podrá depender del CISO directamente, siempre y cuando su alcance sea exclusivo a los procesos vinculados a la SI de la organización. Si su alcance fuese mayor, se recomienda que la misma dependa del COO o CEO de la organización, además de establecer una jerarquía de trabajo lateral o funcional entre el responsable del área de procesos y los siguientes roles de seguridad: CISO, CIPO y SOO.

PM1.1.5	Nivel A	F
Macroproceso de gestión de procesos		
Todos los procesos de negocio de la organización vinculados a la SI deberán ejecutarse a través de un motor de procesos. Para lo cual la organización deberá contar con una herramienta de software BPMS.		

PM1.1.6	Nivel A	F
Macroproceso de gestión de procesos		
El diseño de los procesos de negocio de la organización deberá basarse en el enfoque de arriba hacia abajo. Por lo que su concepción deberá bajar a tierra tanto la estrategia organizacional como su modelo de negocio. Para ello, la organización deberá diseñar y mantener constantemente actualizado un mapa de macroprocesos de SI como mínimo hasta el correspondiente nivel 3. Los procesos de negocio de seguridad deberán encontrarse vinculados al mapa de macroprocesos de SI de la organización.		

PM2 Mejora continua de SI

PM2.1 Programa de mejora continua & compliance de SI

Objetivo Establecer los lineamientos del programa de mejora continua en Seguridad de la Información. A su vez, se enfocará en el establecimiento de directivas de compliance para la seguridad de la organización.

PM2.1.1	Nivel E	F
Proceso de requerimientos		
La organización deberá identificar, documentar y mantener actualizados todos los requisitos: a) Legales. b) Regulatorios. c) Reglamentarios. d) Estatutarios y del negocio. e) Contractuales. f) De mercado. Los requisitos comprenden a todos aquellos vinculados a la organización por su naturaleza de negocio, por sus localizaciones geográficas, sus sistemas de información o sus activos de información.		

Se deberá identificar toda la legislación o documentación externa aplicable vinculada a cada requerimiento identificado por la organización.
ISO 27.001 A.18.1.1 [1]

PM2.1.2	Nivel D	F
Subproceso de registros		
Se deben proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado o divulgación no autorizada, de acuerdo con todos los requisitos identificados en PM2.1.1. La protección deberá ser diseñada en función de la clasificación de sensibilidad correspondiente de cada registro.		
ISO 27.001 A.18.1.3 [1] – ISO 27.002 18.1.3 [14]		

PM2.1.3	Nivel D	F
Macroproceso de compliance		
La organización deberá asegurar la privacidad y la protección de la información personal (“*personal identifiable information*”), según lo requiera la legislación y regulación pertinente, cuando corresponda. Para lo cual la organización deberá: a) Diseñar, establecer y mantener una política de protección y privacidad de la información personal. b) Comunicar la política de protección y privacidad de la información personal y sus lineamientos a todo el personal (propio, contratista o de terceras partes) de la organización.		
ISO 27.001 A.18.1.4 [1] – ISO 27.002 18.1.4 [14]		

PM2.1.4	Nivel D	F
Macroproceso de compliance		
La organización deberá identificar, revisar periódicamente y documentar los requisitos para que los acuerdos de confidencialidad reflejen las necesidades de la organización respecto a la protección de su información. Los acuerdos de confidencialidad deberán abordar los requisitos de protección de la información confidencial utilizando términos legales exigibles y encontrarse adecuadamente documentados por el tiempo que la organización considere adecuado. A su vez, los acuerdos de confidencialidad deberán cumplir con todas las leyes y regulaciones aplicables para la jurisdicción en la cual se apliquen. Los acuerdos de confidencialidad son aplicables tanto a las partes externas como a los empleados de la organización. Los requisitos para los acuerdos de confidencialidad deben revisarse periódicamente, así como también cuando ocurran cambios que influyan sobre dichos requisitos.		
ISO 27.001 A.13.2.4 [1] – ISO 27.002 13.2.4 [14]		

PM2.1.5	Nivel C	F
Macroproceso de compliance		
La organización deberá implementar los procedimientos apropiados para asegurar el cumplimiento de los requisitos identificados en PM2.1.1 relacionados con los derechos de propiedad intelectual y el uso de productos de software propietarios. Para lo cual la organización deberá tener en cuenta los siguientes lineamientos: a) El diseño, implementación y mantenimiento de una política de cumplimiento del derecho de propiedad intelectual que defina el uso legal de los productos de información y de software. b) Adquirir software únicamente a través de fuentes conocidas y con reputación, para garantizar que no se viole el derecho de propiedad intelectual.		

c) Comunicar y capacitar a todo el personal sobre los lineamientos de protección de los derechos de propiedad intelectual.
d) Establecer procesos formales de notificación y toma de acciones disciplinarias contra el personal que incurra en incumplimientos a la política establecida en a).
e) El mantenimiento de registros adecuados de activos y la identificación de todos los activos que requieran protección de los derechos de propiedad intelectual.
f) El mantenimiento de las pruebas y la evidencia de la propiedad de las licencias, discos maestros, manuales, etc.
g) La implementación de controles para garantizar que no se exceda el máximo número de usuarios permitidos por la licencia.
h) La verificación de que se instalen solamente software autorizado y productos licenciados.
i) El establecimiento de una política para el mantenimiento de las condiciones apropiadas de la licencia.
j) El establecimiento de una política para la disposición final o transferencia de software a otros.
k) El cumplimiento de los términos y las condiciones con respecto al software e información obtenidos de redes públicas.
l) Impedir la copia, la conversión a otro formato o la extracción de registros comerciales (películas, audio) u otros que no estén permitidos por la legislación sobre derechos de autor.
l) Impedir la copia total o parcial de libros, artículos, reportes u otros documentos, excepto los permitidos por la legislación sobre derechos de autor.

ISO 27.001 A.18.1.2 [1] – ISO 27.002 18.1.2 [14]

PM2.1.6	Nivel C	F

Macroproceso de compliance

La organización deberá utilizar los controles criptográficos cumpliendo todos los acuerdos, leyes y regulaciones pertinentes. Para ello deberá considerar:

a) Las restricciones sobre la importación o la exportación de hardware y software para realizar funciones criptográficas.
b) Las restricciones sobre la importación o la exportación de hardware y software diseñado para posibilitar el agregado o incorporación de funciones criptográficas.
c) Las restricciones sobre el uso del cifrado.

d) Los métodos requeridos por las autoridades del país para controlar el acceso discrecional u obligatorio a la información cifrada por hardware o software, a fin de proveer la confidencialidad del contenido.

Se recomienda buscar asesoramiento legal para garantizar el cumplimiento de las leyes y las regulaciones pertinentes.

ISO 27.001 A.18.1.5 [1] – ISO 27.002 18.1.5 [14]

PM2.1.7	Nivel C	F

Subproceso de registros

En función de la protección de los registros, la organización deberá:

a) Almacenar cualquier clave criptográfica y programa asociados con archivos cifrados o firmas digitales para permitir el descifrado de los registros durante todo el tiempo que se los retenga.
b) Considerar la posibilidad de deterioro de los medios utilizados para el almacenamiento de los registros.
c) Diseñar, implementar y mantener los procesos de almacenamiento y manipulación de acuerdo con las indicaciones del fabricante.
d) Diseñar, implementar y mantener los procesos necesarios para garantizar la capacidad de acceso a los datos (la legibilidad tanto del formato como del medio) durante todo el período de retención.
e) Diseñar, implementar y mantener lineamientos para la retención, el almacenamiento, la manipulación y la eliminación de los registros y la información.

ISO 27.002 18.1.3 [14]

PM2.1.8	Nivel C	F

Macroproceso de mejora continua

Se deberán controlar todos los cambios:

a) De la organización.

b) De los procesos de negocio vinculados a la organización.
c) De las instalaciones de procesamiento de información vinculadas a la organización.
d) De los sistemas vinculados a la organización.

El objetivo del presente requerimiento consiste en analizar dichos cambios para así poder determinar si los mismos afectan o no a la SI de la organización (si son o no cambios significativos para la seguridad). De afectarla, se deberán diseñar, implementar y monitorear acciones que aseguren el normal cumplimiento de todos los controles, procesos, políticas y lineamientos del Sistema de Mejora Continua en SI de la organización.

En cuanto a la gestión de dichos cambios significativos, la organización deberá:

e) Identificar dichos cambios y registrarlos adecuadamente.
f) Diseñar, implementar y mantener un proceso formal de aprobación para los cambios propuestos.
g) Verificar que los requisitos de SI se hayan cumplido.
h) Comunicar los detalles del cambio a todas las partes interesadas pertinentes.
i) Establecer los roles y las responsabilidades formales para asegurar el control satisfactorio de todos los cambios.
j) Cuando se realicen cambios, mantener un registro de auditoria que contenga toda la información de este.

ISO 27.001 A.12.1.2 [1] – ISO 27.002 12.1.2 [14]

PM2.1.9	Nivel C	F
Macroproceso de mejora continua		
La organización deberá mejorar continuamente la pertinencia, la adecuación y eficacia del Sistema de Mejora Continua de SI.		
ISO 27.001 10.2 [1]		

PM2.1.9	Nivel C	F
Macroproceso de compliance		
Los requisitos de los acuerdos de confidencialidad establecidos por la organización deberán considerar: a) Una definición de la información a proteger. b) La duración esperada de un acuerdo, incluyendo los casos en los cuales podría ser necesario mantener la confidencialidad indefinidamente. c) Las acciones requeridas cuando se rescinde un acuerdo. d) Las responsabilidades y las acciones de los signatarios para evitar la divulgación no autorizada de la información. e) La propiedad de la información, los secretos comerciales y la propiedad intelectual, y su relación con la protección de la información confidencial. f) El uso permitido de la información confidencial y los derechos del signatario para usar la información. g) El derecho para auditar y monitorear las actividades que involucren información confidencial. h) El proceso para la notificación y el informe de la divulgación no autorizada o de la fuga de información confidencial. i) Los términos para que la información se devuelva o destruya al rescindir el acuerdo. j) Las acciones que se espera llevar a cabo en caso de incumplimiento del acuerdo.		
ISO 27.001 10.2 [1]		

PM2.1.10	Nivel B	F
Macroproceso de mejora continua		
En cuanto a la gestión de cambios, la organización deberá: a) Planificar y ensayar los cambios. b) Evaluar los impactos potenciales, incluyendo los impactos de SI ocasionados por tales cambios. c) Diseñar, establecer y mantener los procesos para la vuelta atrás (“fall back”), incluyendo los procedimientos y las responsabilidades para la suspensión y la recuperación ante cambios no exitosos y eventos imprevistos.		

d) Diseñar, establecer y mantener un proceso de cambios de emergencia para permitir la implementación rápida y controlada de los cambios necesarios urgentes.
ISO 27.002 12.1.2 [14]

PM2.1.11	Nivel B	F
Macroproceso de mejora continua		
La organización deberá mejorar continuamente a su vez, la eficiencia del Sistema de Mejora Continua de SI.		

PM2.1.12	Nivel B	F
Subproceso de registros		
En función de la protección de los registros, la organización deberá: a) Mantener un inventario de fuentes de información clave. b) Establecer un cronograma de retención, identificando los registros y el período de tiempo durante el cual se los debe retener. c) Implementar un sistema de almacenamiento y manipulación garantice la identificación de los registros y de su período de retención tal como lo definan las leyes o regulaciones nacionales o regionales, si corresponde.		
ISO 27.002 18.1.3 [14]		

[Página dejada en blanco intencionalmente]

Anexo II

Nueva versión piloto del MRU

El presente capítulo del TFM se enfocará en detallar la nueva versión piloto del MRU. En la misma se detalla principalmente la identificación de nuevas interrelaciones entre requerimientos y documentación fuente del MRU. A continuación, se incluirán únicamente aquellos requerimientos que han sido modificados en esta nueva versión. Cabe resaltar que toda vez que el TFM se refiera a un requerimiento que ha sido mejorado, la referencia apunta específicamente a los requerimientos incluidos en el presente capítulo.

AII.1 Nueva versión del Subsistema Gobierno de Seguridad

Ajustar el requerimiento GOB1.2.3 de la siguiente forma:

GOB1.2.3	Nivel C	F
Ajustar el requerimiento GOB1.2.3.a reemplazándolo con el siguiente texto: a) Asegurarse que requisitos del SMCSI de la organización se encuentren integrados a los procesos existentes y futuros de la organización.		

Ajustar el requerimiento GOB1.3.6 reemplazando al mismo por el siguiente:

GOB1.3.6	Nivel C	F
Subproceso de Revisión del SMCSI		
El órgano rector de gobierno de la organización deberá dirigir las revisiones del Sistema de Mejora Continua de SI a través de la implementación del requerimiento GOB1.3.4. La dirección ejecutiva debe revisar el Sistema de Mejora Continua de SI de la organización a intervalos planificados para asegurar que continúa siendo pertinente, adecuado y eficaz. La revisión del SMCSI por parte de la dirección ejecutiva deberá incluir consideraciones sobre: a) El estado de las acciones tomadas en función de revisiones previas. b) Los cambios internos y externos pertinentes al Sistema de Mejora Continua de SI y a la SI de la organización. c) La retroalimentación de las partes interesadas. d) Los resultados y la performance de la evaluación del riesgo de SI y el estado del plan de tratamiento del riesgo de SI. e) Las oportunidades de mejora continua. f) La retroalimentación sobre el desempeño de la SI, incluyendo, pero no limitándose a: *I. Los resultados de auditoria.* *II. Las no conformidades y sus acciones correctivas.* *III. Los resultados del seguimiento y las mediciones de SI.* *IV. El logro de los objetivos de SI.* La salida del subproceso de Revisión del SMCSI deberá de incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio al SMCSI. Se deberá de conservar información documentada como evidencia de la ejecución del presente subproceso y como evidencia de los resultados de las revisiones por parte de la dirección.		
ISO 27.001 9.3 [12]		

Ajustar el requerimiento GOB1.4.3 de la siguiente forma:

GOB1.4.3	Nivel D	F
Ajustar el requerimiento GOB1.4.3.a reemplazándolo con el siguiente texto: a) Ser responsable de la planificación, desarrollo y mejora de la gestión de riesgos vinculados a los activos de información de la organización (su objetivo consistirá en asegurarse que dichos riesgos se encuentren dentro de un nivel aceptable para la organización, por lo que deberá definir y gestionar un plan de gestión del riesgo de SI). El EGR será responsable por la implementación de la gestión de riesgos y los distintos RRs serán responsables por la aceptación de los niveles residuales de riesgos individuales en función del apetito de riesgo definido por el órgano de gobierno de la organización (referirse a GR1.1.3). Ajustar el requerimiento GOB1.4.3.f reemplazándolo con el siguiente texto: f) Informar sobre el rendimiento del SMCSI a la dirección ejecutiva.		

Ajustar el requerimiento GOB1.4.4 de la siguiente forma:

GOB1.4.4	Nivel C	F
Ajustar el requerimiento GOB1.4.4 adicionando el siguiente texto: j) Informar sobre el rendimiento del SMCSI al CSI, a la dirección ejecutiva y al órgano rector de gobierno de la organización. Ajustar el requerimiento GOB1.4.4 reemplazando su último párrafo por el siguiente texto: Los requerimientos de SI mencionados en e) incluirán: l) Los requerimientos legales, reglamentarios, contractuales, estatutarios, del negocio y del mercado que la organización, sus socios comerciales, sus proveedores de servicios y sus contratistas deben cumplir. m) El ambiente sociocultural de la organización, sus socios comerciales, sus proveedores de servicios y sus contratistas. n) Objetivos estratégicos y estrategias generales de negocio de la organización. o) Las necesidades de protección de la SI de la organización.		

p) La gestión de riesgos de SI de la organización de la organización.
q) El conjunto de principios, objetivos y requisitos de negocio para la manipulación, el procesamiento, el almacenamiento, la comunicación y la preservación de la información que la organización ha desarrollado para apoyar sus operaciones.

Ajustar el requerimiento GOB1.4.6 de la siguiente forma:

GOB1.4.6	Nivel C	F
Ajustar el requerimiento GOB1.4.6.k reemplazándolo con el siguiente texto: k) Supervisar la gestión de riesgos de SI de la organización. Por lo que será el responsable de identificar a los RRs y de supervisar el diseño, ejecución y mejora del plan global de gestión de riesgos de SI.		

Ajustar el requerimiento GOB1.4.8 de la siguiente forma:

GOB1.4.8	Nivel C	F
Ajustar el requerimiento GOB1.4.8.e reemplazándolo con el siguiente texto: e) Ser actualizados regularmente y cuando corresponda (por ejemplo, luego de la ocurrencia de alguno de los eventos detallados en GR1.1.2).		

Ajustar el requerimiento GOB1.4.9 de reemplazando al mismo por el siguiente:

GOB1.4.9	Nivel C	F
Macroproceso de dirección estratégica de la SI Subproceso de establecimiento de objetivos de SI		
Al planificar como lograr sus objetivos de SI, la organización deberá determinar: a) Que es lo que se va a hacer. b) Que recursos se van a necesitar. c) El responsable de dicha implementación. d) Tiempos estimados de logro. e) Forma de medición y evaluación de los resultados.		

Debemos recordar que el PESI será el instrumento del CISO para el logro de los objetivos de SI. Por lo tanto, este requerimiento establece los lineamientos a tener en cuenta a la hora de planificar el logro de estos objetivos de SI y de esta forma establece un marco de acción para el correspondiente diseño tanto de la estrategia de SI como el PESI. A través del PESI la organización cumple con el requisito 8.1 de la norma ISO 27.001 [1] al "implementar planes para lograr los objetivos de SI" [1].
GOB2.1.4
ISO 27.001 8.1 [3]

Ajustar el requerimiento GOB2.3.1 de la siguiente forma:

GOB2.3.1	Nivel C	F
Ajustar el requerimiento GOB2.3.1 agregando al mismo el siguiente texto: La organización deberá determinar y proporcionar los recursos necesarios para el diseño, establecimiento, implementación, mantenimiento y mejora continua de su Sistema de Mejora Continua de SI.		
Adicionar como documentación fuente lo siguiente: ISO 27.001 7.1 [1]		

AII.2 Mejoras al Subsistema Lineamientos de Seguridad

Ajustar el requerimiento LS1.1.1 reemplazando al mismo por el siguiente:

LS1.1.1	Nivel E	F
Subproceso de generación del contexto externo		
Se deberá establecer el contexto externo de la organización, el cual debe considerar: a) El contexto político, social y cultural, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo internacional, regional, nacional y local. b) Valores y percepciones de las partes interesadas externas, y las relaciones de la organización con los mismos. c) Tendencias y factores claves que influencian o pudieran influenciar los objetivos de la organización. A su vez, deberá considerar todo otro aspecto relativo al contexto externo que pueda llegar a afectar la capacidad de la organización para desarrollar, implementar, ejecutar y mantener su SMCSI. *El establecimiento del contexto externo es un input clave a la hora de desarrollar el criterio de apetito de riesgo de la organización (GR1.1.3). De esta forma, la organización podrá asegurarse que en todas sus decisiones tiene en cuenta los objetivos y las necesidades de las partes interesadas externas a la misma.* *Se basa principalmente en el contexto global de la organización. No obstante, debe tomar en considerar aspectos específicos relativos a compliance (leyes o regulaciones), necesidades específicas de las partes interesadas, entre otros.*		
LS1.1.3 – LS1.1.4 – GR1.1.3		
ISO 27.001 4.1 [1] – ISO 31.000 4.3.1, 5.3.1 y 5.3.2 [6]		

Ajustar el requerimiento LS1.1.2 reemplazando al mismo por el siguiente:

LS1.1.2	Nivel E	F
Subproceso de generación del contexto interno		
Establecer el contexto interno de la organización, el cual deberá considerar: a) Gobierno, estructura organizacional, roles y responsabilidades. b) Los objetivos estratégicos de la organización y las estrategias elaboradas para alcanzarlos. c) Capacidades de la organización en términos de recursos o conocimiento (Recursos Humanos, capital, tecnología, entre otros). d) Cultura y valores de la organización. e) Procesos y flujos de información, tanto formales como informales. d) Normas, guías, marcos de referencia y estándares adoptados por la organización. e) Alcance y tipos de relaciones contractuales. f) Sistemas de información de la organización. g) Valores y percepciones de las partes interesadas internas, y las relaciones de la organización con los mismos. h) Las políticas de la organización. *El establecimiento del contexto interno es una tarea clave que la organización deberá encarar con seriedad, ya que será este el que moldeará la forma en la que gestionará sus riesgos.*		
LS1.1.3 - LS1.1.4		
ISO 27.001 4.1 [1] – ISO 31.000 5.3.3 y 4.3.1 [6]		

Ajustar el requerimiento LS1.1.3 reemplazando al mismo por el siguiente:

LS1.1.3	Nivel E	F
Proceso de generación del contexto		
Se debe determinar, en función del contexto generado en los requerimientos LS1.1.1 y LS1.1.2: a) Las partes interesadas afectadas por el SMCSI.		

b) Los requisitos de esas partes interesadas identificadas vinculados a la SI. Los requisitos detallados en b) incluirán todos los requerimientos legales, reglamentarios, contractuales y de mercado que corresponda. *El presente requerimiento en conjunto con LS1.1.1 y LS1.1.2 conforma el proceso de generación del contexto de la organización. El cual será de gran utilidad a la hora de diseñar el PESI (GOB2.1.4), gestionar riesgos (GR1.1.6), diseñar el SMCSI de la organización (GOB2.3) y por consecuente todas las actividades de SI.*
LS1.1.1 - LS1.1.2 – GOB2.1.4 – GR1.1.6
ISO 27.001 4.2 [1] – ISO 31.000 5.3 [6]

Ajustar el requerimiento LS1.1.5 de la siguiente forma:

LS1.1.5	Nivel E	F
Ajustar el requerimiento GOB2.3.1 agregando al mismo el siguiente texto: El Sistema de Mejora Continua en SI deberá incluir: a) La información documentada requerida por los requerimientos del MRU. b) La información documentada que la organización considere necesaria para la eficacia del Sistema de Mejora Continua en SI. Al crear y actualizar información documentada, la organización deberá asegurar que su identificación y descripción sea apropiada (por ejemplo: título, fecha, autor o número de referencia), el formato (por ejemplo: lenguaje, versión del software o gráficos) y el medio. La información documentada deberá ser revisada y aprobada respecto de su pertinencia y adecuación.		
Adicionar como documentación fuente lo siguiente: ISO 27.001 7.5.1 [1] Adicionar como documentación fuente lo siguiente: ISO 27.001 7.5.2 [1]		

Ajustar el requerimiento LS1.1.9 reemplazando al mismo por el siguiente:

LS1.1.9	Nivel C	F
Proceso de generación del contexto		
El proyecto de implementación del Sistema de Mejora Continua de SI de la organización deberá ser diseñado, implementado, gestionado y mejorado en función de un enfoque orientado a procesos según lo establecido dentro del Subsistema de Seguridad Procesos y Mejora Continua.		
ISO 27.001 4.4 [1]		

Adicionar el siguiente requerimiento como LS1.1.12:

LS1.1.12	Nivel C	F
Proceso de diseño del SMCSI		
La organización deberá diseñar, adaptar, combinar, implementar, ejecutar, controlar y mejorar los procesos de negocio necesarios para cumplir los requisitos del Sistema de Mejora Continua de SI. Dichos procesos de negocios vinculados a la SI deberán encontrarse documentados para así facilitar la tarea de monitorear que los mismos se ejecuten según como han sido planeados. A su vez, deberá controlar los cambios aplicados y revisar periódicamente las consecuencias de cambios no intencionales, tomando las acciones necesarias para mitigar cualquier efecto adverso, cuando corresponda. La organización deberá asegurarse que se determinen y controlen los procesos provistos por terceras partes.		
ISO 27.001 8.1 [1]		

Adicionar el siguiente requerimiento como LS1.1.13:

LS1.1.13	Nivel C	F
Proceso de diseño del SMCSI		
La información documentada requerida por el Sistema de Mejora Continua de SI y por los requerimientos del MRU relativos al estadio de madurez objetivo de la organización y estadios inferiores deberá ser controlada para asegurar que: a) Se encuentre disponible y apta para su uso, cuando y donde sea necesario. b) Se encuentre adecuadamente protegida (por ejemplo: contra pérdida de confidencialidad, uso inapropiado, pérdida de integridad o su indisponibilidad). c) Su distribución, acceso, recuperación y uso. d) Se gestionen y controlen sus cambios (por ejemplo: la implementación de un control de versiones). e) Sea almacenada, conservada y preservada adecuadamente (incluyendo la preservación de su legibilidad). f) Su disposición final, al término de su vida útil. La organización deberá identificar de modo apropiado y controlar la información documentada de origen externo, que sea considerada necesaria para la planificación y operación del Sistema de Mejora Continua de SI. El acceso detallado en c) hace referencia al permiso de solo lectura o al permiso de lectura y modificación de la información documentada.		
ISO 27.001 7.5.3 [1]		

Ajustar el requerimiento LS1.2.1 de la siguiente forma:

LS1.2.1	Nivel D	F
Ajustar el requerimiento LS1.2.1 agregando al mismo el siguiente texto: La PSI deberá ser aprobada y firmada por la máxima autoridad de la organización.		
Adicionar como documentación fuente lo siguiente: ISO 27.002 5.1.1 [14]		

Ajustar el requerimiento LS1.2.3 de la siguiente forma:

LS1.2.3	Nivel C	F
Ajustar el requerimiento LS1.2.3.j reemplazándolo con el siguiente texto: j) Incluir el compromiso de la organización para la mejora continua de la SI de la organización y para la asignación de recursos para el diseño, implementación, mantenimiento y mejora del Sistema de Mejora Continua de Seguridad de la Información de la organización. Ajustar el requerimiento LS1.2.3.t reemplazándolo con el siguiente texto: t) Abordar los requisitos: I. Creados por la estrategia de negocio de la organización. II. Legales, regulatorios, contractuales, estatutarios y de mercado. III. Creados por el entorno actual y proyectado de amenazas de SI. Ajustar el requerimiento LS1.2.3 agregando al mismo el siguiente texto: u) Estar disponible como información documentada para todas las partes interesadas internas y, a su vez, a las externas cuando corresponda en función de lo estipulado en el requerimiento LS1.2.10. v) Establecer el marco de referencia de gobierno de SI de la organización establecido en GOB1.1.1.		

Ajustar el requerimiento LS1.2.5 de la siguiente forma:

LS1.2.5	Nivel C	F
Ajustar el requerimiento LS1.2.5 agregando al mismo el siguiente texto: e) Estar disponibles como información documentada para todas las partes interesadas internas y, a su vez, a las externas cuando corresponda en función de lo estipulado en el requerimiento LS1.2.10. Ajustar el requerimiento LS1.2.5 agregando al mismo el siguiente texto:		

Si cualquiera de las políticas de seguridad de la organización fuera distribuida a partes externas, se deberá tener cuidado para evitar la divulgación de información sensible o confidencial.

Los responsables de las políticas detallados en d) deberán revisar las políticas a su cargo en forma periódica y a su vez, evaluar regularmente oportunidades de mejora de estas.

Cabe resaltar que el requerimiento LS1.2.6 ha sido erróneamente numerado como "LS1.2.10" dentro del TFE, favor de referirse a la página 117 de dicho documento [2]. Ajustar el requerimiento LS1.2.6 de la siguiente forma:

LS1.2.6	Nivel C	F
Ajustar el requerimiento LS1.2.6 agregando al mismo el siguiente texto: *Las acciones de comunicación y capacitación deberán encuadrarse dentro del Programa de toma de conciencia, entrenamiento y difusión de la SI de la organización.*		

Ajustar el requerimiento LS1.3.1 de la siguiente forma:

LS1.3.1	Nivel C	F
Ajustar el requerimiento LS1.3.1.c reemplazándolo con el siguiente texto: c) Se contemple la posibilidad de colusión entre partes interesadas con responsabilidades y autoridad asignadas por la organización, durante el diseño de los controles de SI. Ajustar el requerimiento LS1.3.1 agregando al mismo el siguiente texto: *Es posible que para las pequeñas organizaciones la aplicación del presente requerimiento sea una tarea significativamente compleja. No obstante, el principio de segregación de tareas y roles debe aplicarse en la medida que sea posible para la organización.*		

La segregación de funciones deberá implementarse en conjunto con actividades de monitoreo, trazas o pistas de auditoria y actividades de supervisión de la gestión de estas.
Adicionar como documentación fuente lo siguiente: ISO 27.002 6.1.2 [14]

Ajustar el requerimiento LS1.3.2 reemplazando al mismo por el siguiente:

LS1.3.2	Nivel C	F
Proceso de definición de la estructura de SI Subproceso de vínculos externos		
Se deberán de establecer y mantener los contactos apropiados con las autoridades pertinentes, con el objetivo de facilitar y simplificar el reporte, análisis y resolución de incidentes de SI), la continuidad y contingencia de los activos de información de la organización y la adaptación de la organización a nuevos cambios legales, regulatorios o de mercado vinculados a la SI. Se deberán de establecer contactos con: a) El CERT nacional y local. b) Organismos regulatorios pertinentes a la naturaleza de las actividades de la organización. c) Los servicios de emergencia (Fuerzas de Seguridad locales, cuerpos de bomberos locales, entre otros). d) Proveedores de servicios esenciales (electricidad, agua, telecomunicaciones, entre otros). e) Organizaciones dedicadas a la lucha contra el Cibercrimen y/o a la Ciberseguridad. f) Organizaciones dedicadas a la formación, capacitación y/o toma de conciencia en materia de SI, Cibercrimen y/o Ciberseguridad y, a su vez, todos aquellos grupos de interés especial, asociaciones profesionales y foros de especialistas en materia de SI. *Debido a la naturaleza y tamaño de la organización a) y e) podrán ser optativos para las implementaciones del SMCSI de aquellas organizaciones cuyo estadio de madurez sea inferior al nivel "B".*		

Si la organización es considerada una infraestructura crítica[49], en función de la Directiva 2008/114/CE del Consejo de la unión Europea [48], o contiene una de las áreas clasificadas como AES[50] por el MRU, todos los apartados del presente requerimiento adquieren carácter obligatorio. *Se recomienda establecer acuerdos o convenios de intercambio de información con el objetivo de mejorar la cooperación y la coordinación ante posibles eventos e incidentes de SI. Dichos acuerdos deberán identificar requerimientos para la protección de la confidencialidad de la información intercambiada.*
ISO 27.001 A.6.1.3 y A.6.1.4 [3] - ISO 27.002 6.1.3 y 6.1.4 [7]

Ajustar el requerimiento LS2.1.3 de la siguiente forma:

LS2.1.3	Nivel C	F
Ajustar el requerimiento LS2.1.3 agregando al mismo el siguiente texto: k) Los RRs (Responsables de Riesgos). Ajustar el requerimiento LS2.1.3 agregando al mismo el siguiente texto: Las responsabilidades de cada autoridad de SI deberán encontrarse documentadas en la Política de Autoridades de SI. A su vez, se deberá documentar el compromiso de la organización para la asignación de la autoridad necesaria para llevar adelante dichas responsabilidades. El personal asignado como autoridad de SI deberá ser competente y poseer experiencia en dicha área. A su vez, la organización deberá brindarles continuamente posibilidades para mantenerse actualizados.		

[49] Según la Directiva 2008/114/CE del Consejo de la unión Europea una infraestructura critica es *"el elemento o sistema esencial para el mantenimiento de las funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar económico o social de la población"* [48].
[50] Áreas de Extrema seguridad. Favor de referirse a la sección 3.1 del presente trabajo.

Ajustar el requerimiento LS2.1.8 de la siguiente forma:

LS2.1.8	Nivel D	F
El requerimiento LS2.1.8 permanecerá tal cual como fue detallado dentro del TFE a excepción que se degradará su nivel de madurez. Por lo tanto, el requerimiento LS2.1.8 pasara a conformar los requerimientos fundamentales del nivel "D" del Modelo de Madurez de SI.		

Adicionar el siguiente requerimiento como LS2.1.14:

LS1.1.14	Nivel C	F
Proceso de establecimiento de autoridades de SI Subproceso de RRs		
La organización deberá establecer un Responsable de Riesgo (RR) para cada uno de los riesgos identificados en GR2.2. Los RRs deberán poseer tanto la responsabilidad como la autoridad para gestionar los respectivos riesgos que les han sido asignados. Los RRs deberán cumplir con todas sus responsabilidades detalladas en GR1.2.3 y, a su vez, serán responsables (junto con el RMO como coordinador gerencial) de la ejecución del proceso de gestión de riesgos de SI. *Se recomienda que los RRs sean seleccionados en función de su conocimiento del negocio. La selección de estas autoridades de seguridad e la información no debe circunscribirse únicamente al personal de las áreas de riesgos, seguridad o TI, sino que debe enfocarse en aquellos tomadores de decisión dentro del negocio.* *Los RRs deberán aceptar las responsabilidades por la gestión de los riesgos que le han sido asignados. Dicha aceptación deberá ser documentada por la organización. A su vez, deberá encontrarse detallada en las descripciones del puesto.*		
GR1.2.3		
ISO 31.000 4.3.3 y Anexo A.3.2 [6] - ISO 31.000 4.3.3 y 4.1 [6] – – ISO 27.001 6.1.2 y 6.1.3 [3] – ISO 31.000 Introducción –		

Adicionar el siguiente requerimiento como LS2.2.22:

LS1.1.14	Nivel C	F
Proceso de definición de la estructura de SI		
La organización deberá implementar una estructura de seguridad que contemple los siguientes lineamientos: a) Establecimiento de un CISO como gerente global de la SI de toda la organización. b) Establecimiento de un RMO. c) Establecimiento de RRs.		

Ajustar el requerimiento LS2.1.6 de la siguiente forma:

- Estableciendo al mismo como requerimiento clave para el nivel D+.

Ajustar el requerimiento LS2.3.3 de la siguiente forma:

LS2.3.3	Nivel E	F
Ajustar el requerimiento LS2.3.3.a reemplazándolo con el siguiente texto: a) Un responsable por dicho Activo de Información. Ajustar el requerimiento LS2.3.3 reemplazando su cuarto párrafo por el siguiente texto: *Todo Activo de Información debe tener un Responsable asignado, los cuales se encargaran de garantizar que los Activos de Información a su cargo reciban un apropiado nivel de protección. Los responsables detallados en a) son aquellos denominados como RAI por los estadios de madurez superiores del MRU.* Ajustar el requerimiento LS1.2.3 agregando al mismo el siguiente texto:		

Las clasificaciones establecidas en c) y d) deberán realizarse en función de lo establecido en LS2.3.6.
Adicionar como requerimiento vinculado el siguiente: LS2.3.6

Ajustar el requerimiento LS2.3.3 de la siguiente forma:

LS2.3.3	Nivel E	F
Ajustar el requerimiento LS2.3.3.a reemplazándolo con el siguiente texto: a) Un responsable por dicho Activo de Información. Ajustar el requerimiento LS2.3.3 reemplazando su cuarto párrafo por el siguiente texto: *Todo Activo de Información debe tener un Responsable asignado, los cuales se encargaran de garantizar que los Activos de Información a su cargo reciban un apropiado nivel de protección. Los responsables detallados en a) son aquellos denominados como RAI por los estadios de madurez superiores del MRU.* Ajustar el requerimiento LS1.2.3 agregando al mismo el siguiente texto: Las clasificaciones establecidas en c) y d) deberán realizarse en función de lo establecido en LS2.3.6.		
Adicionar como requerimiento vinculado el siguiente: LS2.3.6		

Ajustar el requerimiento LS2.3.6 de la siguiente forma:

LS2.3.6	Nivel C	F
Ajustar el requerimiento LS2.3.6 agregando al mismo el siguiente texto: El esquema de clasificación de Activos de Información deberá ser consistente a lo largo de todas sus ejecuciones. *Se debe tener en cuenta que una sobreclasificación (clasificación de activos de información como sensibles cuando estos ya han tomado notoriedad pública) podría ocasionar perdidas tanto económicas como de tiempo a la organización. A*		

su vez, una subclasificación podría poner en peligro el logro de los objetivos estratégicos dela organización.

Ajustar el requerimiento LS2.3.10 de la siguiente forma:

LS2.3.10	Nivel C	K
Ajustar el requerimiento LS2.3.10 agregando al mismo el siguiente texto: El proceso de designación deberá asegurar el establecimiento de un RAI para cada activo de información que se incorpore a la organización (tanto fuera un activo transferido a la organización o creado por la misma). Cada RAI será responsable de implementar el requerimiento LS2.3.6 para cada uno de los Activos de Información que posea a su cargo.		

A su vez, estableciendo al mismo como requerimiento clave para el nivel D+.

Ajustar el requerimiento LS2.3.13 de la siguiente forma:

LS2.3.13	Nivel C	F
Ajustar el requerimiento LS2.3.13 reemplazando su primer párrafo por el siguiente texto: El CSI definirá los niveles de clasificación de los Activos de Información de la organización en función de lo establecido en LS2.3.6. Dichos niveles deberán encontrarse incluidos en la Política de Gestión de Activos que el CISO deberá de desarrollar en función de los requerimientos detallados en los dominios de SI LS2.2 y LS2.3.		
Adicionar como requerimiento vinculado el siguiente: LS2.3.6		

Ajustar el requerimiento LS2.3.14 de la siguiente forma:

LS2.3.14	Nivel C	F
Ajustar el requerimiento LS2.3.14 reemplazando su referencia incorrecta al requerimiento LS2.3.8 por la referencia correcta al requerimiento LS2.3.13.		
Modificar el requerimiento vinculado al siguiente: **LS2.3.13**		

Ajustar el requerimiento LS2.3.15 de la siguiente forma:

LS2.3.15	Nivel C	F
Ajustar el requerimiento LS2.3.15 reemplazando su referencia incorrecta al requerimiento LS2.3.8 por la referencia correcta al requerimiento LS2.3.13.		
Adicionar como requerimiento vinculado el siguiente: **LS2.3.6**		

[Página dejada en blanco intencionalmente]