Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

*Carrera de Especialización en Seguridad Informática*

Trabajo Final de Especialización

# Marco de Referencia Unificado en Seguridad de la Información


Autor: Lic. Lucas Falivene

Tutor: Dr. Pedro Hecht

Marzo 2018

*Cohorte: 2017*

[Página dejada en blanco intencionalmente]

# LICENCIA

Queda hecho el depósito que establece la Ley 11.723.

1° Edición – Marzo 2018 – 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.

# DECLARACION JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales 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.

Lic. Lucas I. Falivene
DNI 37.376.682

## 0.1 Resumen ejecutivo

El presente Trabajo Final de Especialización se enfoca en detallar las bases principales del Marco de Referencia Unificado en Seguridad de la Información (en adelante, MRU). El cual tiene como objetivo brindar un marco de referencia holístico[1] y práctico para todos aquellos que deseen alcanzar un nivel óptimo en materia de Seguridad de la Información, a medida de su propia organización. El Marco de Referencia se encuentra dirigido a compañías públicas y privadas, instituciones y entes públicos, asociaciones sin fines de lucro y cualquier otro tipo de organización que desee alcanzar la mejora continua en Seguridad de la Información. El MRU facilitará significativamente a las organizaciones el cumplimiento de sus objetivos estratégicos y su misión, a través de la disminución al máximo posible los riesgos de seguridad asociados al activo más preciado que poseen: su información.

Las bases de dicho Marco de Referencia se enfocarán en normas, marcos teóricos, manuales, estándares y guías internacionales de Seguridad de la Información. La meta principal del presente trabajo radica en realizar un aporte al mundo de la Seguridad de la Información, no solo a través de la simplificación y centralización de estándares y normas en la materia, sino en la creación de una complementación e integración entre ellos que posibilitará:

- El establecimiento de un nuevo y holístico[1] Modelo de Madurez de Seguridad de la Información, que simplificará significativamente a las organizaciones el camino a recorrer para alcanzar la mejora continua en Seguridad de la Información.
- La medición ágil y efectiva de las acciones de Seguridad de la Información y sus respectivos resultados y beneficios brindados a la organización.

[1] Holístico: "*Del todo o que considera algo como un todo*" [51]. El término aquí utilizado hace referencia al alcance del presente trabajo que, pretende alcanzar a las normas más significativas en la materia.

- El aumento de la eficacia y eficiencia de las organizaciones, por ende, logrando la disminución de costos y la mejora significativa de la seguridad y la performance de la organización.

A su vez, el MRU combinará los requerimientos de toda la documentación fuente[2] mencionada anteriormente con la metodología de gestión de procesos. Esto último permitirá optimizar la eficiencia y la eficacia de todos los procesos relativos a la seguridad de la información de la organización.

Por último, el objetivo final del presente trabajo consiste en establecer las bases de un Sistema de Mejora Continua en Seguridad de la Información basado en un marco de referencia holístico que a largo plazo, podría de tomarse como puntapié inicial para la creación de un nuevo estándar dentro del mundo de la Seguridad de la Información.

*Palabras claves*

Estándares Internacionales, Procesos de Negocio, Calidad, Mejora Continua, Mejores Prácticas, Difusión & Entrenamiento, Involucramiento del Recurso Humano, Enfoque en el Negocio, Gestión de Riesgos, Modelo de Madurez de Seguridad de la Información.

[2] Término utilizado en el presente trabajo para englobar a todos los estándares, normas, marcos teóricos, manuales y guías internacionales de Seguridad de la Información que han sido consultadas.

## 0.2 Índice de contenidos

# 1

# Introducción al MRU

Poco a poco las organizaciones descubren la importancia de lograr la mejora continua en Seguridad de la Información, muchas a consecuencia de haber sufrido significativas pérdidas a causa de numerosos ataques e incidentes de seguridad tanto internos como externos. El Marco de Referencia Unificado en Seguridad de la Información (MRU) persigue como objetivo final la prevención de tales situaciones, logrando así una disminución significativa de los costos vinculados a incidentes de seguridad y una valiosa mejora en la efectividad de la organización.

La variada cantidad de estándares, normas, guías y marcos teóricos referentes a la Seguridad de la Información complejizan enormemente la tarea de búsqueda e implementación de los mejores marcos de referencia[3] en la materia. El objetivo del MRU consiste en simplificar dicha tarea y dotar a las organizaciones de un macro-proceso (proceso genérico que podrá modificarse a medida[4]), de la implementación de un Sistema de Mejora Continua en Seguridad de la Información basado en un único Marco de Referencia –el MRU– y en el Modelo de Madurez de Seguridad de la Información, lo que guiará, referenciará y simplificará el trabajo de todas las organizaciones de forma significativa.

[3] Conocidos generalmente como *"Frameworks"* en inglés. Los marcos de referencia funcionan en forma de guía conceptual para el logro de un objetivo específico, en este caso el de gestionar la seguridad.
[4] Dicho macro-proceso podrá modificarse a medida gracias a la incorporación de la metodología de gestión por procesos. La misma se encuentra detallada en la sección 1.6 del presente trabajo.

El MRU toma en consideración múltiples estándares, marcos teóricos, manuales, guías y normas internacionales vinculadas a la Seguridad de la Información y a la calidad de los procesos de Seguridad de la Información. **De esta forma, logra centralizar, simplificar y establecer una integración y complementación entre todos los requerimientos necesarios para lograr la mejora continua en materia de Seguridad de la Información, adaptada a cada organización, en un único marco de referencia.**

## *1.1 Alcance*

El MRU brinda un marco de referencia holístico[5] y práctico para todos aquellos que deseen alcanzar un estadio de madurez de mejora continua en materia de Seguridad de la Información. Dada la complejidad del tema seleccionado, el presente Trabajo Final de Especialización se enfocará únicamente en los lineamientos estructurales y primordiales del MRU. Por lo que, se sentaran las bases del mismo:

- Se definirá la estructura del MRU (como se clasificarán y detallaran sus requerimientos) y sus requerimientos principales.
- Se detallará la documentación que ha sido utilizada como fuente para el desarrollo del MRU.
- Se desarrollará el Modelo de Madurez de Seguridad de la Información, realizando énfasis en sus niveles y su interrelación con el MRU y la documentación fuente[6].
- Se desarrollará el Sistema de Mejora Continua en Seguridad de la Información y se detallarán todos los Subsistemas que lo componen.

[5] Holístico: "*Del todo o que considera algo como un todo*". Hace referencia al alcance del presente trabajo que, pretende alcanzar a las normas más significativas en la materia.
[6] Término utilizado en el presente trabajo para englobar a todos los estándares, normas, marcos teóricos, manuales y guías internacionales de Seguridad de la Información que han sido consultadas.

- Se diseñarán en forma completa los Subsistemas de Gobierno de Seguridad de la Información y Lineamientos de Seguridad de la Información, como objetivo del Trabajo Final de Especialización.

## *1.2 Orígenes*

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[7], con el objetivo de facilitar la implementación de los macro-procesos de mejora continua de Seguridad de la Información, por parte de cualquier organización. Entre los estándares, marcos teóricos, normas, guías y marcos de referencia internacionales considerados, se encuentran los siguientes:

- ISO[8] 9.001 [6] e ISO 9.000 [5]: normas internacionales de calidad.
- ISO/IEC 27.001 [2] [3], ISO/IEC 27.002 [7], ISO/IEC 27.003 [18], ISO/IEC 27.004, ISO/IEC 27.005 [8], ISO/IEC 27.006 [9], ISO/IEC 27.007 [10] e ISO/IEC 27.000 [1]: normas internacionales de Seguridad de la Información.
- ISO/IEC 27.014 [12]: estándar internacional sobre gobierno corporativo de Seguridad de la Información.
- Metodología de Seguridad de la Información de la NSA[9] [19].
- Manuales y guías técnicas de seguridad diseñadas por la NSA [20].
- Manuales y guías de seguridad diseñadas por el Departamento de Seguridad Interior de los EEUU [21].
- Marco de Trabajo COBIT[10] [22].
- Directrices de la OCDE[11] para la Seguridad de la Información [49].

[7] Término utilizado en el presente trabajo para englobar a todos los estándares, normas, marcos teóricos, manuales y guías internacionales de Seguridad de la Información consultadas. Las mismas pueden encontrarse en la sección bibliográfica del Trabajo Final de Especialización.
[8] Organización Internacional de Normalización.
[9] Agencia de Seguridad Nacional de los EEUU.
[10] Objetivos de control para la información y tecnologías relacionadas.
[11] Organización para la Cooperación y el Desarrollo Económico.

- Los principios de seguridad generalmente aceptados establecidos por el Comité del GASSP[12] [25].
- ISO 31.010 [29] e ISO 31.000 [28]: corresponden a la Gestión de Riesgos.
- ISO 22.301: estándar internacional sobre el Sistema de Gestión de la Continuidad [30].
- Directiva de Seguridad de la Información 8570.1 – M del Departamento de Defensa de los EEUU [35].
- Estándar de clasificación TIER[13] para Data Centers del Uptime Institute [17].
- El estándar de buenas prácticas del ISF[14] [41].

## *1.3 Propósito*

El propósito fundamental del presente trabajo radica en: facilitar y mejorar la compleja experiencia a la que todos aquellos profesionales de Seguridad de la Información se enfrentan a la hora de relevar e implementar múltiples estándares y normas en la materia, en sus respectivas organizaciones. Por lo que el MRU propone convertirse en una herramienta del profesional de seguridad que permita, a través de la centralización y simplificación de toda su documentación fuente, agilizar significativamente el proceso de implementación de las mejores prácticas en Seguridad de la Información.

El presente trabajo final tiene a su vez como objetivos:

- Sentar las bases primordiales del Marco de Referencia Unificado en Seguridad de la Información (MRU).
- Permitir al cursante obtener un nivel de conocimiento profundo sobre aquellas temáticas vinculadas a la Gestión Estratégica de la Seguridad de la

[12] Principios de Seguridad de Sistemas Generalmente Aceptados, por sus siglas en ingles.
[13] El estándar evalúa Data Centers en función de su infraestructura, en términos de los requerimientos del negocio de disponibilidad del sistema. [17]
[14] #*Information Security Forum*" por sus siglas en ingles. En español: Foro de Seguridad de la Información.

Información y, un nivel de conocimiento significativo sobre temáticas vinculadas a los aspectos técnicos de la Seguridad de la Información.

- Crear, desarrollar y establecer una metodología de trabajo que permita concretar la centralización, clasificación, relacionamiento y creación de complementación e integración entre toda la documentación fuente considerada por el MRU.

En cuanto a los objetivos del MRU podemos recalcar los siguientes:

- Facilitar significativamente a las organizaciones el cumplimiento de sus objetivos estratégicos y su misión, a través de la disminución al máximo posible los riesgos asociados al activo más preciado que poseen: su información.
- Prevención de ataques, amenazas e incidentes de seguridad tanto internos como externos, logrando así una disminución significativa de los costos vinculados a incidentes de seguridad y una valiosa mejora en la efectividad de la organización. A su vez, pretende preservar la imagen, reputación y confianza pública de la organización, al lograr prevenir la obtención de prensa y fama negativa a causa de un ataque de Seguridad.
- La creación e implementación de un Modelo de Madurez holístico y pragmático que simplifique y guie el camino hacia el logro de la mejora continua en Seguridad de la Información, por parte de cualquier tipo de organización.
- Recopilación, clasificación y vinculación de las normas, estándares y marcos teóricos y de referencia de Seguridad de la Información más reconocidos internacionalmente, con el objetivo de identificar y documentar las vinculaciones entre ellos que permitan armonizar los distintos requerimientos del MRU y, de esta forma, crear una complementación e integración única.

- Proporcionar conciencia y capacitar sobre la importancia de la Seguridad de la Información y el respeto a la privacidad.
- Proveer referencia y convertirse en una fuente de conocimientos libre y gratuita para todos los profesionales vinculados a la Seguridad de la Información.

El Marco de Referencia Unificado en Seguridad de la Información está dirigido a:

- Compañías públicas y privadas, instituciones y entes públicos, asociaciones sin fines de lucro y cualquier otro tipo de organización que desee alcanzar un estadio de madurez de mejora continua en materia de Seguridad de la Información.
- Profesionales de seguridad que deseen comprender y conocer el MRU con el objetivo de mejorar su conocimiento y adoptar un nuevo marco de referencia holístico y pragmático en la materia.
- Estudiantes en busca de material para sus trabajos de investigación y de estudio.

## *1.4 Criterio de selección de normas y estándares*

Durante la primera etapa del presente trabajo, correspondiente al relevamiento de la Documentación Fuente del MRU, se realizó una investigación a fondo de todos aquellos documentos potenciales que podrían llegar a ser incorporados. En un principio, la tarea no implico demasiado esfuerzo, ya que se comenzó con aquellos documentos más reconocidos en la temática. No obstante, una vez establecidos los primeros documentos, comenzaron a surgir otros que no poseían una visión fundamentalmente estratégica sobre la Seguridad de la Información, sino que mencionaban o la desarrollaban desde otro ángulo (como por ejemplo desde el punto de vista de la Tecnología Informática), eran extremadamente específicos (por lo que contrastaban con el alto nivel de abstracción

necesario para el desarrollo del MRU) o simplemente contenían un abundante detalle técnico, por lo que no concordaban con la visión estratégica del presente trabajo.

Se arribó entonces a la conclusión de que se debía de establecer un criterio para la selección de aquellos documentos potenciales a ser relevados. A través del mismo, se escogerían los documentos que serían efectivamente tomados como fuente para el desarrollo del Trabajo Final de Especialización. El criterio consistió en seleccionar todas aquellas normas vinculadas en mayor medida a un enfoque de gestión (por lo que se descartan aquellas normas técnicas puras) y que posibiliten la interconexión de requerimientos con otras normas a un nivel de abstracción claramente estratégico (por lo que se priorizan las normas de la serie ISO 27.000, COBIT, ISF y similares).

Una vez establecido el criterio, se procedió a realizar la selección de los documentos que integran la documentación fuente del MRU. Dicha selección se encuentra detallada en la sección bibliográfica del presente trabajo, para un análisis más detallado por parte del lector.

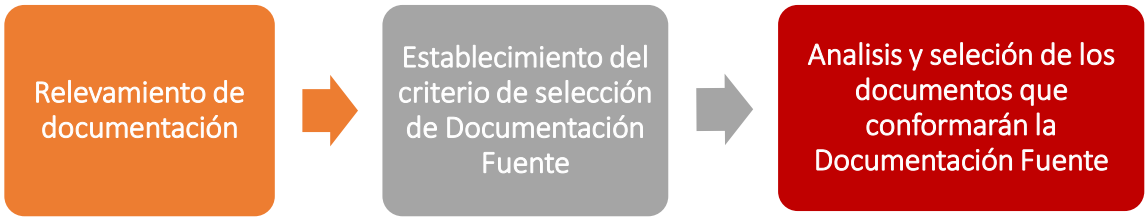



**Ilustración 1.4.1: Proceso relevamiento y selección de la Documentación Fuente.**

Por último, cabe resaltar que se ha realizado un planeamiento en función de la documentación fuente seleccionada, clasificando las normas que serán implementadas en forma total o parcial dentro del Trabajo Final de Especialización. El mismo se basó en el criterio de alcance del presente trabajo: el diseño en forma completa los Subsistemas de Gobierno de Seguridad de la Información y Lineamientos de Seguridad de la Información.

## *1.5 Metodología de relevamiento, centralización e integración*

El primer paso realizado para la construcción del Sistema de Mejora Continua en Seguridad de la Información, consistió en el relevamiento de todos los índices de contenidos de los documentos que conformaban la documentación fuente. Dichos listados han sido clasificados y ordenados individualmente en grupos de temáticas en función del alcance establecido por la ISO 27.001 [3]. Una vez finalizado dicho relevamiento, se detectó que ciertos grupos podrían llegar a fusionarse entre sí con el objetivo de facilitar la lectura y comprensión del lector. Como resultado del paso anterior han surgido las 9 categorías de Seguridad que conformarán el Sistema de Mejora Continua en Seguridad dela Información del MRU.

Una vez establecidos estas 9 categorías, se procedió a ejecutar e iterar el siguiente proceso con cada uno de los documentos que componen la Documentación Fuente:

1. Selección de un documento.
2. En el caso que se trate de una implementación parcial:
    a. Lectura y análisis completo de la documentación seleccionada con el objetivo de localizar todas aquellas temáticas inherentes al alcance establecido para el Trabajo Final de Especialización.
3. En el caso que se trate de una implementación completa:
    a. Lectura y análisis completo de la documentación con el objetivo de localizar todas las temáticas relevadas de la misma dentro de las categorías establecidas anteriormente.
4. Volcado de las temáticas relevadas al MRU, en un formato de requerimiento dentro de la categoría correspondiente.

La primera iteración del proceso se realizó de forma sencilla y sin sobresaltos, ya que consistió en una mera organización y clasificación de los requerimientos del primer documento (la norma ISO 27.001 [3]). No obstante, al comenzar a ejecutar el proceso en función de la segunda documentación fuente, la dificultad aumento considerablemente debido a:

- La necesidad de clasificación de los requerimientos en forma que optimice e intente alcanzar la homogeneidad a lo realizado en la iteración previa del proceso.
- La necesidad de lograr fusionar los requerimientos de las distintas documentaciones fuente de manera que se logre establecer una complementación e integración entre estas (analizando detalladamente las relaciones de los distintos documentos con el objetivo de identificar aquellos puntos que se contraponen, difieren, complementan o se superponen).

La dificultad continúo aumentando significativamente con cada documento adicionado.

Se incluye a continuación, a modo de ejemplo, un requerimiento del MRU, con el objetivo de que el autor pueda comprender y advertir de forma simple la complementación e integración creada por el presente trabajo:

> El Marco de Referencia de gobierno de Seguridad de la Información deberá abordar la necesidad de:
>
> a) Coordinar todas las actividades de Seguridad de la Información de la organización.
> b) Asegurarse que dichas actividades mencionadas en a) sean integrales e integradas a la organización.
> c) Coordinar de forma ágil y precisa las actividades relacionadas con la Seguridad de la Información, primordialmente aquellas vinculadas con la seguridad física.
> d) Establecer la responsabilidad sobre la Seguridad de la Información en toda la gama de actividades de la organización. Se deberá integrar y especificar dicha responsabilidad a los roles de la organización, por ejemplo a través del establecimiento de Responsables de Activos de Información, Responsables Gerenciales y otras autoridades establecidas por el MRU (favor de referirse al requerimiento LS2.2).
>
> *Se debe prestar especial atención al establecimiento de la responsabilidad en los vínculos con las partes interesadas, aquellas secciones percibidas como "fronteras" o "limites" de la organización, como por ejemplo la información almacenada por un proveedor de servicios de almacenamiento en la "nube".*

| *Bibliografía en la que se basa el presente requerimiento:* |
| --- |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.1 [12] |

**Ilustración 1.5.1: ejemplo de requerimiento de seguridad de la información del MRU.**

Para la creación de dicho requerimiento se han fusionado y creado una complementación e integración entre los siguientes requerimientos:

- Las autoridades de Seguridad de la Información (Responsables de Activos de Información, Responsables Gerenciales, entre otras) establecidas por el MRU se basan en una denominación propia, en función del alcance y responsabilidades de las diferentes autoridades contenidas en la documentación fuente y, a su vez, incorporando algunas variaciones de producción propia. Esto último ilustra claramente la metodología que se ha utilizado durante la realización del presente Trabajo Final de Especialización.
- El requerimiento 5.4.1 de la norma ISO 27.014 [12] desglosado y, a su vez, combinado con los requerimientos SG1.1.4, SG1.1.5 y SG1.1.6 del estándar del ISF [41]. Dichos elementos fueron combinados con una cierta producción propia y luego, entrelazados al proceso de diseño y creación del Marco de Referencia de gobierno de Seguridad de la Información, mediante la conformación del subproceso de Organización y Responsabilidades. Esto último ilustra claramente la metodología de gestión por procesos que se ha utilizado durante la realización del presente Trabajo Final de Especialización.

Una vez volcados los requerimientos de toda la documentación fuente alcanzada por el Trabajo Final de Especialización, se procedió a dividirlos a discreción con el objetivo de amoldarlos al Modelo de Madurez de Seguridad de la Información. Por lo que, un requerimiento con diversas directivas se transformará en distintos requerimientos individuales, que clasificarán las directivas del requerimiento padre original en función de los niveles del Modelo de Madurez. Esto último se realiza con el objetivo de mapear los requerimientos de la documentación fuente a los distintos estadios de madurez del MRU,

para allanar y establecer, de esta forma, la guía hacia la mejora continua en Seguridad de la Información.

Luego de constituidos los distintos estadios de madurez asociados a los requerimientos, se procedió a la definición y establecimiento de los procesos de Seguridad de la Información asociados a cada uno de ellos.

## *1.6 Gestión por procesos & MRU*

El MRU toma en consideración el enfoque de Gestión por Procesos de Negocios. La misma consiste en "*una disciplina de gestión que involucra cualquier combinación de modelado, automatización, ejecución, control, medición y optimización de flujos de trabajo empresarial*" [13], en concordancia con el cumplimiento de los objetivos estratégicos del negocio y *"en funcionamiento conjunto con los sistemas, empleados, clientes y socios dentro y fuera de la organización"* [13]. Dicha metodología tiene como objetivo principal *"mejorar tanto la eficacia como la eficiencia de las actividades de la organización a través de la optimización y automatización de sus procesos de negocio"* [14].


**Ilustración 1.6.1: Detalle de la misión de la gestión por procesos del MRU.**

El MRU incorpora la metodología de Gestión por Procesos de Negocios con el objetivo de dotar a las organizaciones de una disciplina que permita traducir las políticas MRU en sus correspondientes procesos de negocio (comúnmente conocidos como

flujogramas[15]). De esta forma la capacitación y la implementación del MRU se tornan significativamente más sencillas y por lo tanto más rápidas. La metodología actuará en el último eslabón del Marco de Referencia del MRU (favor de referirse a la sección 3.4 del presente trabajo) facilitando la vinculación de las políticas con los procesos, permitiendo de esta forma "bajar a tierra" lo establecido en dichos documentos en un proceso de negocio.

### ¿Qué es un proceso?

En función de lo detallado en la norma ISO 9.000 [5], un proceso es *"conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados"* [5]. Para facilitar la comprensión del lector, se realizará una descripción gráfica tomando el ejemplo del proceso de *clasificación de activos de información* establecido por el MRU (favor de referirse a la ilustración 1.6.2). Se puede observar las múltiples actividades del proceso (ilustradas en formato de "rectángulos azules") que simbolizan las distintas tareas que el personal debe realizar para alcanzar una correcta clasificación de activos de información. Por lo tanto, podemos decir que un proceso es un mapa (simbolizado en un flujograma, como aquel incluido en la ilustración 1.6.2), que enmarca y guía nuestro trabajo.

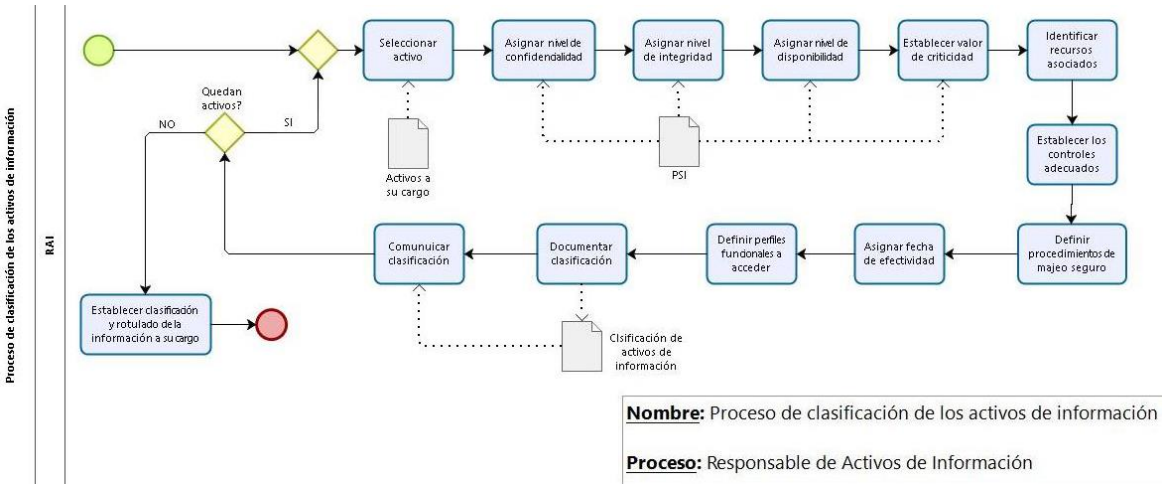



**Ilustración 1.6.2: Proceso de clasificación de activos de información.**

[15] Vale la pena realizar énfasis en detallar que el flujograma es solo un componente más del proceso de un negocio.

Para los RRHH no vinculados a la Seguridad de la Información, siempre les resultará mucho más sencillo la lectura del flujograma de un proceso, que la lectura de un procedimiento o norma de seguridad. Esto se debe a que la documentación del proceso ha sido específicamente diseñada para facilitar su comprensión y correspondiente capacitación, en función de una disminución significativa del nivel de abstracción. Los procesos logran traducir paso a paso el flujo de trabajo a seguir para cumplir con todos los controles y requerimientos del MRU, siempre y cuando los mismos se encuentren diseñados e implementados de forma correcta. Las políticas describen requerimientos globales y poco específicos mientras que un proceso describe actividades específicas con mayor nivel de detalle. Por este motivo, el personal de la organización no tendrá necesidad de realizar una lectura minuciosa de los procedimientos, normas y guías de seguridad establecidas, sino que simplemente se dedicará a analizar sus actividades particulares y especificas dentro del proceso que deberá desarrollar, simplificando así significativamente la capacitación necesaria en materia de Seguridad de la Información.

¿Qué beneficios se obtienen con la Gestión por Procesos?

- Mayor visibilidad de las actividades de Seguridad de la Información de la organización.
- Documentación estandarizada de todas las actividades y operaciones relativas a la Seguridad de la Información.
- La adecuación del área de seguridad a los requerimientos de la norma ISO 9.001.
- Significativa disminución en los tiempos de capacitación de RRHH y en la ejecución de los procesos de negocio. De esta forma, la metodología de Gestión por Procesos de Negocio mejorará de forma sustancial la eficiencia de las actividades de Seguridad de la Información de la organización.
- Mejora significativa de la eficacia y eficiencia de las actividades de Seguridad de la Información de la organización, al disminuir considerablemente los tiempos de interrelación entre las distintas áreas funcionales intervinientes en el proceso y, al

eliminar toda posibilidad de duda o desconocimiento de las responsabilidades y obligaciones del personal de la organización.

- Mejora de los procesos de inducción del nuevo personal de la organización, simplificándolos y acortando significativamente su lapso temporal.

Otra ventaja de la adopción de la metodología de Gestión por Procesos radica en la facilidad de implementación y adopción de cambios. Aplicar modificaciones a los procesos resulta significativamente más sencillo que aplicarlos a diversas políticas aisladas, ya que la misma metodología nos permitirá visualizar rápidamente los alcances y efectos de dichos cambios. Lo que a su vez, influenciará positivamente a la hora de la gestión del cambio y capacitación de los RRHH.

Cada proceso contiene 2 componentes primordiales: su flujograma y su correspondiente documentación (tanto de ALTO como de BAJO nivel). La documentación de ALTO nivel posee un nivel de abstracción mayor y tiene como objetivo establecer un marco y guía para la ejecución total del proceso. En cambio, la documentación de BAJO nivel posee un nivel mínimo de abstracción y tiene como meta describir y explicar – a través de imágenes, tablas y/o cuadros – como, cuando y porque realizar cada una de las actividades del proceso. Puede observarse las diferencias entre los tipos de documentación de procesos en la siguiente tabla:

| TIPO DE DOCUMENTACIÓN | NIVEL DE ABSTRACCIÓN | CANTIDAD | ¿QUÉ EXPLICA? | LECTOR OBJETIVO |
|---|---|---|---|---|
| ALTO Nivel | Alto | 1 | El proceso en su conjunto | Responsable del proceso |
| BAJO Nivel | Muy bajo | Depende de la cantidad de roles del proceso | Cada actividad del proceso en forma individual | Roles que ejecutan cada una de las actividades |

**Tabla 1.6.1: diferencias entre la documentación de ALTO y BAJO nivel.**

La ilustración 1.6.2 nos permite visualizar el proceso de clasificación de activos de información del MRU. La correspondiente visualización gráfica conforma un lenguaje, una notación, conocida como BPMN 2.0[16] (Modelo y Notación de Procesos de Negocio). Podemos definir al lenguaje BPMN como *"una notación gráfica y estandarizada que permite el modelado de los procesos de negocio, en formato de flujo de trabajo (workflow)"* [42].


**Ilustración 1.6.3: jerarquía de traducción de políticas del MRU.**

La metodología de Gestión por Procesos de Negocio consiste en traducir los procesos de la organización al estándar BPMN 2.0. De esta forma, el motor de procesos – el software de la metodología BPM, conocido como BPMS[17]: Sistema de Gestión de Procesos de Negocio – logra comprender y ejecutar la lógica de negocio utilizada por la organización. En otras palabras, la Gestión por Procesos traduce las actividades de la organización a un lenguaje estándar que un determinado software, el motor de procesos específicamente, logra comprender.

La clave de la metodología sujeta a análisis recae en remplazar la generación de código con la actividad de modelar procesos. De esta forma, los RRHH no técnicos podrán diseñar las aplicaciones de negocios con una eficacia y eficiencia actualmente inmejorables.

[16] *"Business Process Model and Notation"* por sus siglas en inglés.
[17] *"Business Process Management Systems"* por sus siglas en ingles.

## ¿Por qué es necesario un software BPMS?

Los procesos de negocios son en general significativamente más complejos que el observado en la ilustración 1.6.2 y, a su vez, contienen múltiples interrelaciones (macroprocesos y subprocesos). Debido a esta complejidad, se requiere de un software que colabore en las tareas del personal estableciendo una guía para su trabajo, centralizando las comunicaciones (documentos, expedientes, correos electrónicos, etc.) y recordando que acciones debe de realizar y como es que las debe de llevar a cabo. Es por esta razón que el motor de procesos impactará significativamente en la eficacia y eficiencia de las actividades de Seguridad de la Información de la organización.

La implementación de un Sistema de Gestión de Procesos de Negocio (BPMS) requiere de un alto compromiso de la organización en cuanto a recursos y, principalmente, un claro enfoque en la gestión del cambio, ya que viraríamos de un enfoque funcional a uno orientado a procesos. Es por ese motivo, que el MRU requiere de la adopción e implementación de un Sistema de Gestión de Procesos de Negocio, únicamente en su estadio de madurez más exigente.

## Procesos de Negocio & ECM

Si combinamos la metodología de Gestión de Procesos de Negocio con software de las categorías BPMS (Sistemas de Gestión de Procesos de Negocio, el cual permite ejecutar los procesos de negocio) y ECM (Gestión de Contenidos Empresariales, el cual tiene como objetivo *"estructurar y organizar la forma de almacenar los documentos tales como archivos, informes y expedientes de la organización"* [15]) se facilitan de forma significativa las actividades de la organización, disminuyendo al mínimo la necesidad y tiempos de capacitación de RRHH relativos a inducción o a cambios en los procesos, eliminando actividades ineficientes e innecesarias, estableciendo y documentando claramente las funciones y responsabilidades de cada rol, implementando un registro de todas las actividades y documentos creados, facilitando el camino hacia la despapelización y enmarcando y guiando el trabajo de todo el personal de la organización.

La gestión por procesos colisiona con la visión general de la operación funcional de las organizaciones, es por este motivo que el MRU requiere de su implementación completa abarcando por lo menos el total de los procesos de la organización susceptibles de presentar aspectos o requerimientos de Seguridad de la Información, únicamente para alcanzar los mayores estadios de madurez del MRU.

[Página dejada en blanco intencionalmente]

# 2

# Estrategia MRU

El MRU basa todos sus requerimientos en el cumplimiento en forma conjunta de 7 principios estratégicos fundamentales para lograr la mejora continua en Seguridad de la Información:


**Ilustración 2.1: principios estratégicos del MRU.**

- Enfoque orientado en el negocio: el objetivo final de la Seguridad de la Información consiste en facilitar el cumplimiento de los objetivos estratégicos del negocio, a

través de una efectiva gestión de riesgos de sus activos de información. Los recursos y esfuerzos destinados a la seguridad tienen un impacto decisorio sobre el logro o incumplimiento de los objetivos estratégicos de negocio, ya que definen la efectividad del área de Seguridad de la Información de proteger la creación de valor de la organización, morigerando la destrucción de valor causada por los incidentes de Seguridad de la Información.

- Mejores Prácticas: el MRU toma en cuenta, indexa y prioriza las mejores prácticas vinculadas a la Seguridad de la Información. A su vez, logra crear una complementación e integración única entre ellas, posibilitando a las organizaciones el máximo acercamiento a la mejora continua, en materia Seguridad de la Información.

- Difusión & Entrenamiento: El MRU realiza un significativo hincapié en la importancia del establecimiento del Programa de toma de Conciencia, Entrenamiento y Difusión. Este principio apunta específicamente al primer nivel de defensa de la Seguridad de la Información de cualquier organización: los Recursos Humanos.

- Involucramiento del Recurso Humano: nuevamente otro principio con hincapié en el personal de la organización en cuanto a Seguridad de la Información. El MRU comprende la importancia que significa el involucramiento de los Recursos Humanos antes, durante y después de la implementación, el cumplimiento, el monitoreo y la mejora de los procesos, controles, protocolos y metodologías de Seguridad de la Información adoptadas por la organización.

- Gestión por procesos: los procesos colaboran en el logro de la mejora continua en Seguridad de la Información, al mejorar significativamente la implementación y la efectividad de las actividades de seguridad. A su vez, tienen un impacto significativamente favorable sobre la simplificación y la mejora radical de los procedimientos de capacitación de los Recursos Humanos y gestión del cambio.

- Calidad: el logro de la mejora continua en Seguridad de la Información requiere de controles, procesos, protocolos y metodologías eficaces, eficientes y, sobre todo, medibles.

- Mejora Continua: la Seguridad de la Información muta constantemente, es por esta razón que debemos de estar atentos, capacitarnos continuamente y reforzar periódicamente el nivel de seguridad de nuestras organizaciones. El MRU colabora en el cumplimiento de dicho principio a través de la implementación del Subsistema de Procesos y Mejora Continua[18].

La estrategia MRU es llevada a la práctica por el Sistema de Mejora Continua en Seguridad de la Información, el cual implementa el total de los requerimientos necesarios para alcanzar, en función del MRU, el estadio de madurez de mejora continua en Seguridad de la Información.

## *2.1 Componentes del MRU*

Se procederá a continuación a detallar los grandes elementos que componen el Marco de Referencia Unificado en Seguridad de la Información. Aquellos dos grandes componentes son:

- El Sistema de Mejora Continua en Seguridad de la Información: implementado por el MRU. El mismo contiene todos los requerimientos (controles, buenas prácticas, procesos, procedimientos, etc.) del MRU. Se encuentra dividido en 9 grandes Subsistemas de Seguridad de la Información. El desarrollo en detalle del mismo podrá de encontrarse en el capítulo 3 del presente trabajo.

[18] Dicho Subsistema compone una de las 9 categorías del Sistema de Mejora Continua en Seguridad de la Información detalladas en la sección 1.4 del presente trabajo.

- El Modelo de Madurez de Seguridad de la Información: 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 Seguridad de la Información. Su objetivo es guiar y apoyar a la organización antes, durante y después de la implementación del Sistema de Mejora Continua en Seguridad de la Información. El desarrollo en detalle del mismo podrá de encontrarse en el capítulo 4 del presente trabajo.

Se incluye a continuación una ilustración que sin duda colaborará en el entendimiento de los componentes fundamentales del MRU por parte del lector.


**Ilustración 2.1.1: componentes del MRU.**

[Página dejada en blanco intencionalmente]

# 3

# Sistema de Mejora continua en Seguridad de la Información

Uno de los objetivos del MRU consiste en la implementación de un Sistema de Mejora continua en Seguridad de la Información. El mismo establece todos los requerimientos necesarios (procesos, políticas, protocolos, controles, metodologías, soluciones y mejores prácticas) para que cualquier organización pueda, en función del MRU, alcanzar la mejora continua en Seguridad de la Información.

**Misión del Sistema de Mejora continua en Seguridad de la Información**

*Permitir a las organizaciones alcanzar la Mejora continua en Seguridad de la Información a través del establecimiento de los procesos requeridos, las mejores prácticas, los controles necesarios, del programa de toma de conciencia, entrenamiento y difusión de la Seguridad de la Información y de las soluciones de seguridad que permitan optimizar la efectividad de los objetivos estratégicos de las organizaciones del siglo XXI.*

## *3.1 Subsistemas del Sistema de Mejora Continua en Seguridad de la Información*

El Sistema de Mejora Continua en Seguridad de la Información es desarrollado por el MRU a través de un conjunto de 9 Subsistemas, los cuales engloban las diversas ramas y temáticas de la Seguridad de la Información. De esta forma, los requerimientos del

estado del arte en Seguridad, contenidos por el MRU, se encontrarán agrupados y clasificados dentro de los siguientes 9 Subsistemas:

I. Subsistema de GOBIERNO de Seguridad de la Información: comprende los lineamientos del MRU para un eficaz y eficiente gobierno de Seguridad de la Información.

II. Subsistema de LINEAMIENTOS DE SEGURIDAD: comprende todas las definiciones, reglamentos y protocolos generales en los que se basa el Sistema de Mejora Continua en Seguridad de la información.

III. Subsistema de GESTIÓN de RIESGOS: comprende al módulo específico de relevamiento, identificación, medición y tratamiento de los riesgos a los cuales los activos de información de la organización se encuentran sujetos.

IV. Subsistema de INGENIERÍA DE SEGURIDAD: comprende una lista de los controles, procesos y metodologías generales y específicos de Seguridad de la Información a implementar. A su vez, comprende los requerimientos vinculados a la gestión de incidentes de Seguridad de la Información.

V. Subsistema de GESTIÓN de la TECNOLOGÍA: corresponde a la seguridad integral de los sistemas y, de las operaciones y comunicaciones de la organización vinculados con los mismos.

VI. Subsistema de gestión de los RECURSOS HUMANOS: corresponde a todos los controles y requerimientos vinculados con la primera línea de defensa, en cuanto a Seguridad de la Información, de todas las organizaciones.

VII. Subsistema de GESTIÓN de la CONTINUIDAD: corresponde a los requerimientos vinculados a la recuperación de la información y la continuidad de las actividades de la organización.

VIII. Subsistema de SEGUIMIENTO & CONTROL: corresponde a la auditoría y a la evaluación, cumplimiento y el monitoreo continuo del Sistema de Mejora Continua en Seguridad de la información.

IX. Subsistema de PROCESOS Y MEJORA CONTINUA: corresponde a uno de los elementos más importantes durante la implementación, gestión, mantenimiento y mejora del Sistema de Mejora Continua en Seguridad de la información. El mismo se encuentra centrado en el estado futuro y en la mejora de los procesos de Seguridad de la Información, y no en el día a día de las operaciones de seguridad.


**Ilustración 3.1.1: Subsistemas de Seguridad de la Información. Los subsistemas remarcados corresponden a los desarrollados en el anexo al presente trabajo.**

## *3.2 Organización de los Subsistemas de Seguridad de la Información*

Cada uno de los Subsistemas de Seguridad de la Información contiene una serie de requerimientos a cumplir basados en controles, protocolos, reglas, procesos, metodologías, guías y formas de organización del flujo de trabajo de la Seguridad. Para facilitar su comprensión por parte del lector, los requerimientos serán a su vez clasificados en diversas sub-categorías dentro de los Subsistemas de Seguridad de la Información. La

descripción y desglose de dichas sub-categorías podrán de encontrarse en forma completa dentro del anexo al presente Trabajo Final de Especialización[19].

### *3.3 Mapa parcial de subsistemas del MRU*

Se procederá a continuación a detallar la composición de los correspondientes Subsistemas del Sistema de Mejora Continua en Seguridad de la información, que han sido diseñados para el Trabajo Final de Especialización.

| GOB | Gobierno de Seguridad de la Información |
|---|---|
| GOB.1 | Enfoque de gobierno de Seguridad de la Información |
| GOB.1.1 | Marco de Referencia de gobierno de Seguridad de la Información |
| GOB.1.2 | Principios de Gobierno de Seguridad de la Información |
| GOB1.3 | Macroprocesos de gobierno de Seguridad de la Información |
| GOB1.4 | Dirección estratégica de la Seguridad de la Información |
| GOB.2 | Componentes de gobierno de Seguridad de la Información |
| GOB.2.1 | Estrategia de Seguridad de la Información |
| GOB2.2 | Distribución de valor para las partes interesadas |
| GOB2.3 | Sistema de Mejora continua en Seguridad de la Información |

**Tabla 3.2.1: mapa del Subsistema de Gobierno de Seguridad de la Información.**

[19] Dicha información es incluida en el Anexo con el objetivo de no dificultar la lectura y entendimiento por parte del lector al agregar demasiado detalle a la explicación del Sistema de mejora Continua en Seguridad de la información.

| LS | Lineamientos de Seguridad de la Información |
|---|---|
| LS.1 | Organización general de la Seguridad de la Información |
| LS.1.1 | Contexto de la Organización & Implementación del SMCSI |
| LS.1.2 | Política de Seguridad de la Información |
| LS1.3 | Marco de Referencia para la gestión de la SI |
| LS.2 | Estructura y organización de la Seguridad y de la Información |
| LS.2.1 | Estructura del área de Seguridad de la Información |
| LS2.2 | Estructura de Gobierno de SI |
| LS2.3 | Gestión de activos de Información |

**Tabla 3.2.2: mapa del Subsistema Lineamientos de Seguridad de la Información.**

## *3.4 Marco de Referencia del MRU*


**Ilustración 3.4.1: MRU, de la teoría a la práctica.**

El marco de referencia que gira en torno al MRU se compone de 6 elementos fundamentales estrechamente entrelazados entre sí, basados en un enfoque de arriba hacia abajo, en donde cada uno de ellos se centra en un nivel de abstracción menor que su precedente. Dicha estructura facilita la navegación desde la estrategia en la que se basa el presente trabajo, la rectora del Marco de Referencia Unificado en Seguridad de la Información, hacia la implementación de los procesos de Seguridad de la Información que logran "bajar a tierra" y transformar en tangible la estrategia del MRU.

Dicho Marco de Referencia, se encuentra basado en la metodología de cascada de metas utilizada por COBIT, donde en función de las necesidades de las partes interesadas (insumo primordial de la estrategia del MRU) se delinean en forma de cascada los objetivos corporativos y luego, en base a estos, los objetivos de Seguridad de la Información [22].

## *3.5 Objetivos del Sistema de Mejora Continua en Seguridad de la información*

El Sistema de Mejora Continua en Seguridad de la información, 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 el Sistema de Mejora Continua en Seguridad de la información logra que las organizaciones:

- Obtengan una clara guía de apoyo a su transformación en Seguridad, a través de una serie de requerimientos de Seguridad de la Información orientados al negocio y, clasificados en función del Modelo de Madurez del MRU.
- Obtengan una respuesta ágil y flexible a las constantes amenazas de seguridad que mutan y evolucionan rápidamente a lo largo del tiempo.

- Identifiquen e integren al Sistema de Mejora Continua en Seguridad de la información los distintos requerimientos legales, regulatorios, estatutarios, contractuales y de mercado que deben cumplir.
- Gestionen efectivamente sus riesgos y los disminuyan a los niveles que consideren aceptables, obteniendo así el nivel de Seguridad de la Información apropiado para su organización.

Estos últimos objetivos se desprenden de las metas estratégicas del MRU, las cuales han sido detalladas en la sección 1.3 del presente trabajo.

[Página dejada en blanco intencionalmente]

# 4

# Estadios de madurez MRU

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 Seguridad de la Información conformado 5 estadios de madurez: 4 de estos 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 Seguridad de la Información, en forma completa. De esta forma, gracias al Modelo de Madurez del MRU, se simplifica significativamente el recorrido que las organizaciones deberán de afrontar desde un estadio de *"ignorancia feliz"*[20], hasta lograr optimizarlo alcanzando la mejora continua en Seguridad de la Información. Existen 5 estadios de madurez MRU, cada uno de ellos con sus respectivos requerimientos a cumplir en función de una complejidad ascendente.

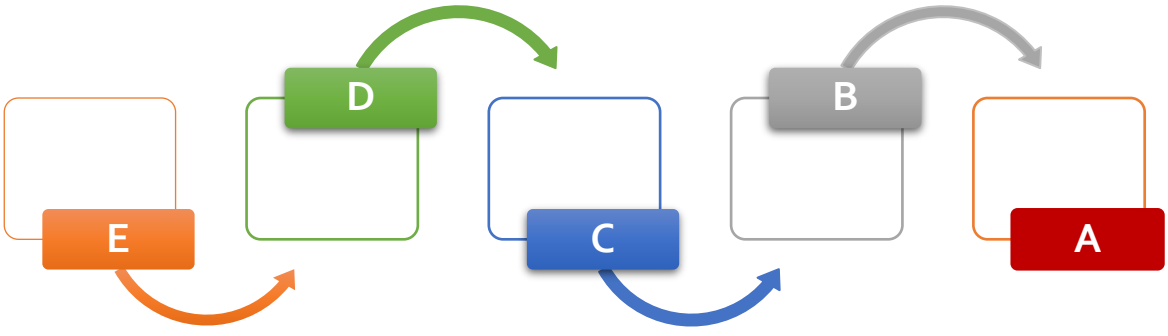



**Ilustración 4.1: estadios de madurez MRU.**

[20] Indica el estadio 0 en cualquier tipo de escala de maduración. Termino extraído de un documento de Gartner relativo a los niveles de maduración del proceso de capacitación de Seguridad de la Información en las organizaciones. [16]

A su vez, se establecen 4 estadios de madurez intermedios, con el objetivo de colaborar y facilitar la evolución de las organizaciones a través del Modelo de Madurez, con la meta final de lograr la mejora continua en Seguridad de la Información. Los niveles intermedios adicionan el símbolo "+" a cada uno de los estadios de madurez. Para lograr alcanzar un nivel intermedio se deberá cumplir con las siguientes dos condiciones:

- Implementación del 20% de los requerimientos básicos[21] del estadio de madurez MRU inmediatamente superior.
- Implementación de todos los requerimientos clave[21] del estadio de madurez MRU inmediatamente superior.

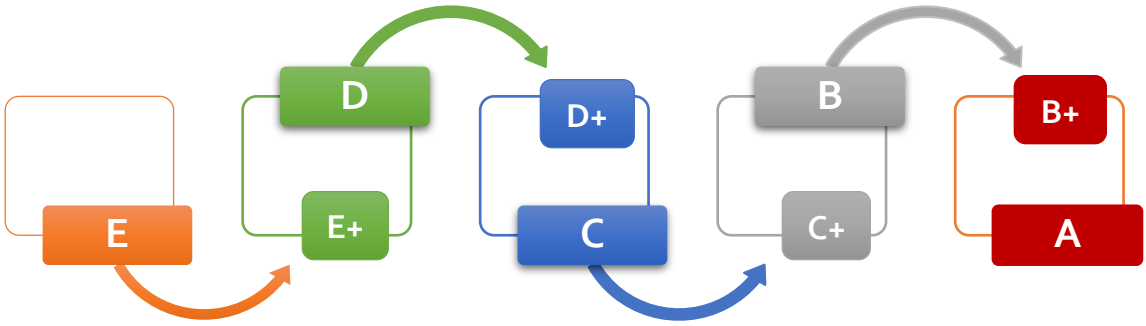



**Ilustración 4.2: estadios de madurez intermedios.**

## *4.1 Modelo de Madurez de Seguridad de la Información*

El segundo componente del MRU, consiste en el Modelo de Madurez de Seguridad de la Información. El objetivo del mismo 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 Seguridad de la Información. Para lograr este objetivo, el Modelo de Madurez del MRU clasifica todos sus requerimientos de seguridad en función de los estadios de

[21] 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 el Anexo al presente trabajo.

madurez detallados anteriormente. A continuación se procederá a detallar los requerimientos fundamentales de cada estadio de madurez MRU, que podrán observarse en la ilustración 4.1.1.

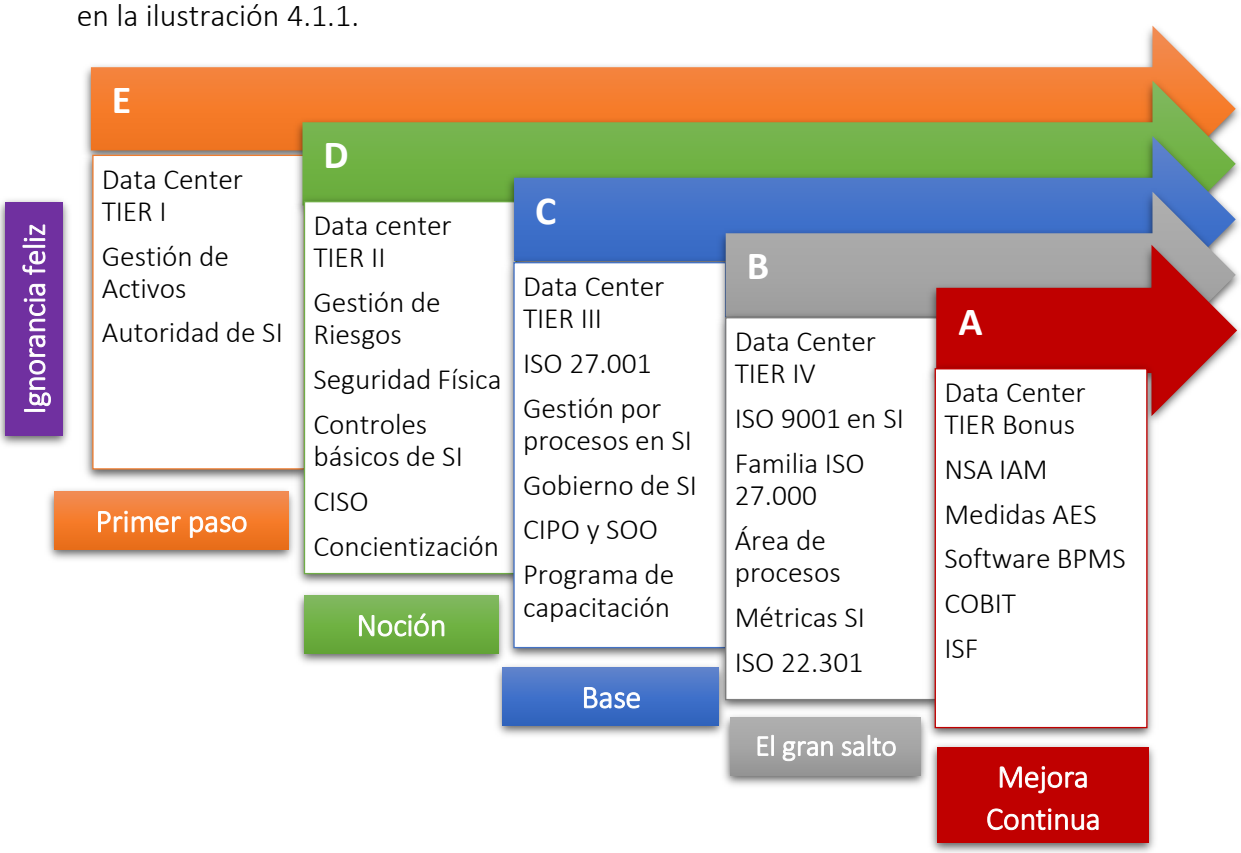



**Ilustración 4.1.1: requerimientos fundamentales en función del estadio de madurez MRU. SI: Seguridad de la Información.**

Puede observarse el nivel creciente en cuanto a complejidad de implementación y gestión de los requerimientos de Seguridad de la Información vinculados a cada estadio de madurez MRU. Cabe resaltar, 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.

El Modelo de Madurez de Seguridad de la Información ha sido específicamente diseñado para guiar el establecimiento de un Sistema de Mejora Continua en Seguridad de la información desde la *"ignorancia feliz"*[22] [16] hacia la mejora continua en Seguridad

[22] Indica el estadio 0 en cualquier tipo de escala de maduración. Termino extraído de un documento de Gartner relativo a los niveles de maduración del proceso de capacitación de Seguridad [16].

de la Información. De esta forma el logro de la implementación en forma completa del Sistema de Mejora Continua en Seguridad de la información por parte de una organización se ve facilitado y simplificado significativamente, ya que solo se debe de seguir los pasos establecidos en dicho modelo, implementando en forma gradual y priorizando los requerimientos del MRU. El Modelo de Madurez de Seguridad de la Información 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 Seguridad de la Información.

El estadio de madurez "F" es considerado aquel relativo a la "*ignorancia feliz*", ya que se encuentra dirigido a todas aquellas organizaciones que no cumplen con los requerimientos mínimos del MRU.

El Modelo de Madurez combina e integra las siguientes variables:

- La madurez de los procesos de Seguridad de la Información de la organización.
- La madurez del programa de toma de conciencia, entrenamiento y difusión de la Seguridad de la Información dentro de la organización.
- La madurez del gobierno de Seguridad de la Información de la organización.
- La madurez de la gestión de riesgos llevada adelante por la organización.
- El grado de madurez de los controles y medidas de Seguridad de la Información implementados por la organización.
- La madurez del Sistema de Mejora Continua en Seguridad de la información de la organización.

## *4.2 Composición de los estadios de Madurez*

Los requerimientos 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 puede dividirse en cuatro etapas:

- Ignorancia feliz: estadio correspondiente a la "Ignorancia Feliz", el mismo incluye a todas aquellas organizaciones que no logran alcanzar el estadio de madurez "E" del MRU.
- Noción de Seguridad de la Información: contiene los estadios "E" y "D". El objetivo de esta etapa consiste en el fortalecimiento de los puntos primordiales y básicos de Seguridad de la Información.
    - El **estadio "E"** se encuentra centrado en el relevamiento e identificación de los activos de información de la organización y en el establecimiento de una autoridad de Seguridad de la Información. El mismo pretende establecer las bases primordiales para la gestión de riesgos (ya que sin conocer los activos de información no nos es posible manejar sus riegos) y la gestión de la Seguridad de la Información de la organización. Constituye el primer paso hacia la mejora continua.
    - El **estadio "D"** se centra principalmente en la gestión de riesgos y en la implementación de controles básicos de seguridad. Aquí se levantará 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 logro de transmitirles la justificación de la inversión en Seguridad de la Información), se iniciarán las primeras acciones de concientización y capacitación en la materia y se establecerá el rol de CISO (punto primordial para la implementación exitosa de estadios superiores). De esta forma se logra establecer una noción de Seguridad de la Información dentro de la organización.
- Base de Seguridad de la Información: contiene el **estadio "C"**. Esta etapa se centra en la implementación de todos los requerimientos base de Seguridad de la Información, 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 [3], 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, requiriendo:

- La implementación de un Gobierno de Seguridad de la Información.
- La gestión por procesos de todas las actividades de la organización vinculadas a la Seguridad y/o sean susceptibles de presentar aspectos o requerimientos de seguridad.
- Diferentes autoridades de Seguridad de la Información 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, entre otras).
- El diseño e implementación de un programa de capacitación continúo en Seguridad de la Información con alcance a toda la organización.

- Mejora Continua en Seguridad de la Información: contiene los estadios "B" y "A". El objetivo aquí radica en el logro de la mejora continua en Seguridad de la Información. Para ello, el Modelo de Madurez guía en la implementación de varios requerimientos complejos, que no podrán ser alcanzados por cualquier tipo de organización.
  - El **estadio "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 [6] 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 Seguridad de la Información. A su vez, dicho estadio requiere de la implementación de las normas más importantes de la

familia ISO 27.000[23] y del estándar de continuidad del negocio ISO 22.301 [30]. Constituye el gran salto desde una base común de Seguridad hacia la mejora continua.

- El **estadio "A"** se centra en el logro de la mejora continua en Seguridad de la Información. Para ello requiere de la implementación de la metodología IAM de la NSA [19], cuyo principal eje se enfoca en el establecimiento de la conocida metodología[24] del equipo rojo y equipo azul. En dicho estadio se pretende implementar en forma completa los lineamientos de buenas prácticas del estándar del ISF [41] y de la sección del marco de trabajo COBIT [22] dirigida a la Seguridad de la Información. 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 seguridad y, a su vez, de las medidas de Áreas de Extrema Seguridad[25] del **MRU**. Constituye el último estadio del Modelo de Madurez del **MRU**.

Por último, se debe resaltar el requerimiento relativo al estándar TIER[26] del Uptime Institute [17]. Cada estadio de madurez del **MRU** se encuentra vinculado con uno de los niveles TIER, siempre en función de la lógica de complejidad ascendente del Modelo de madurez de Seguridad de la Información. Dicho estándar tiene un claro énfasis en la disponibilidad de la infraestructura tecnológica y no en Seguridad, no obstante configura un excelente complemento para los Subsistemas de Gestión de la Tecnología y Gestión de la Continuidad. Vale la pena recalcar que el Modelo de Madurez requiere de la adecuación de todos los Data Center vinculados a la organización, tanto como aquellos

[23] Referenciadas en la bibliografía como [1], [2], [3], [7], [8], [9], [10], [12] y [18].
[24] 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.
[25] 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 la sección7.2 del anexo al presente trabajo.
[26] El estándar evalúa Data Centers en función de su infraestructura, en términos de los requerimientos del negocio de disponibilidad del sistema.

localizados dentro de está (conocidos como "*on-site*" o "*on-premise*") como los contratados o terciarizados (mediante algún mecanismo de "*outsourcing*"), a los requerimientos del Estándar TIER.

## *4.3 Ordenamiento de requerimientos*

En contraste con la norma ISO 27.001 [3], el orden de los requerimientos del MRU refleja no solo su importancia, sino su complejidad de implementación, debido a que los mismos se encuentran clasificados y agrupados en función de los diversos estadios de madurez del MRU (detallándose en primera instancia las principales bases en Seguridad y luego en forma creciente los diversos requerimientos en pos de alcanzar la mejora continua en Seguridad de la Información).

De esta forma, cada Subsistema de Seguridad de la Información contiene todos sus requerimientos clasificados y ordenados en función de un nivel creciente de complejidad de implementación. Por lo que, cada subsistema comenzará con aquellos requerimientos del estadio de madurez "E" y cuando estos se agoten continuará con aquellos correspondientes al estadio "D" y así sucesivamente hasta alcanzar el último nivel.

## *4.4 Certificaciones*

El Sistema de Mejora Continua en Seguridad de la información logra establecer un SGSI [27](Sistema de Gestión de la Seguridad de la Información) [3] en su correspondiente estadio de madurez "C", por lo que de esta forma al implementar dicho estadio de

[27] El SGSI constituye el corazón de la norma ISO 27.001. El objetivo de la mima se centra en la implementación de dicho Sistema de Gestión de la Seguridad de la Información, detallando todos los requerimientos necesarios para su concreción.

madurez, se está cumplimentando a su vez con todos los requisitos para certificar la norma ISO 27.001 [3].

De la misma forma que sucede con la norma ISO 27.001 [3], el MRU comprende la implementación completa de diversos estándares en función de ciertos estadios de madurez MRU. Por lo que, las organizaciones estarán en condiciones de certificar aquellas normas internacionales que integran la Documentación Fuente del presente estándar, si así lo desean.

[Página dejada en blanco intencionalmente]

# 6

# Conclusiones

La realización del presente trabajo requirió del diseño y creación de una metodología de trabajo específica para el relevamiento, indexación e integración de los distintos requerimientos de diversas normas, estándares, marcos teóricos y guías internacionales de seguridad de la Información. Dicha estrategia de trabajo ha sida encarada con el objetivo de combinar, centralizar y crear una complementación e integración entre toda la documentación fuente considerada por el MRU. Esto último, permite disminuir significativamente la complejidad de comprensión y relevamiento de los estándares más reconocidos y aceptados internacionalmente y, simplificar en gran mediada la tarea de implementación de los mismos. De esta forma, el presente Trabajo Final de Especialización logra establecer los primeros pasos de una metodología centrada en facilitar a las organizaciones el logro de la mejora continua en Seguridad de la Información, a través:

- De la incorporación del Modelo de Madurez en Seguridad de la Información a su estrategia de negocio, con el objetivo de guiar la implementación de los diversos requerimientos de Seguridad detallados por el MRU, simplificando de esta forma el camino que cualquier tipo de organización deberá recorrer a través de los distintos estadios de madurez.
- De la incorporación de un enfoque orientado a procesos para el diseño, gestión y mejora de todas las actividades vinculadas a Seguridad de la Información de la organización.

- Del flujo libre de información, convirtiéndose en una fuente de conocimientos libre y gratuita para cualquier profesional vinculado a la Seguridad de la Información.
- El derribo de una complejidad ante la cual todos los profesionales de Seguridad de la Información se encuentran a la hora de alcanzar la mejora continua, a través de la implementación de diversos estándares y normas internacionales en la materia.
- De la creación de una complementación e integración entre toda la documentación fuente considerada, de esta forma satisfaciendo y llevando a un nivel único en la materia los principios 3 y 4 del marco teórico COBIT ("*aplicar un Marco de Referencia Único Integrado*" [22] y "*Hacer posible un Enfoque Holístico*" [22]).

El fin ulterior del MRU recae en simplificar la tarea de los profesionales de Seguridad de la Información, ya que actualmente el desarrollo de cualquier tipo de proyecto considerable de Seguridad en grandes organizaciones se encuentra plagado de múltiples complicaciones y obstáculos. Principalmente, el MRU, se enfoca en morigerar la compleja experiencia por parte del profesional de Seguridad de la Información, a la hora de navegar aquellas implementaciones de proyectos que requieran de la utilización en forma conjunta de diversos estándares y normas en la materia.

Los resultados del presente trabajo constituyen los primeros pasos para la conformación y establecimiento del MRU y su correspondiente Modelo de Madurez de Seguridad de la Información, debido a la significativa complejidad de la materialización de dicho proyecto.

[Página dejada en blanco intencionalmente]

# 7

# Anexo

## *7.1 Abreviaturas utilizadas dentro del anexo*

Durante la realización de los Subsistemas piloto (Gobierno de Seguridad de la Información y Lineamientos de Seguridad de la información) del MRU, se han utilizado los siguientes atajos dentro del desarrollo de los requerimientos de seguridad de la Información:

**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.

**CIPO[28]:** 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 SI requeridas por el SMCSI.

**CISO[29]:** Gerente de Seguridad de la Información, autoridad máxima de SI en la organización.

**CSI:** Comité de Seguridad de la Información, 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.

[28] *"Continuous Improvement & Process Office"*, Oficina de Procesos y Mejora Continua por sus siglas en inglés.
[29] "*Chief Information Security Oficer"*, Gerente de Seguridad de la Información por sus siglas en inglés.

EGR: 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 la misma a corto y largo plazo para las partes interesadas" [22].

MRE: Marco de Referencia del MRU. Se detalla en la sección 3.3 del presente trabajo.

PCED: Programa de toma de Conciencia, Entrenamiento y Difusión del MRU. El mismo se establece dentro del SSI de Recursos Humanos.

PSI: Política de Seguridad de la Información.

RASI: Responsable de Auditoria de SI.

RG: Responsables Gerenciales, todo aquel gerente o titular de un área, división o sección de la organización.

RMO[30]: responsable de riesgos de SI de la organización. Conforma una de las áreas de SI requeridas por el SMCSI.

RP: 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.

SMCSI: Sistema de Mejora Continua en Seguridad de la información.

SOO[31]: responsable del día a día de SI, ya que es quien lleva adelante los procesos tácticos y operativos 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 SI requeridas por el SMCSI.

[30] *"Risk Management Office"*, Oficina de Gestión de Riesgos por sus siglas en inglés.
[31] "*Security Operations Office"*, Oficina de Operaciones de Seguridad por sus siglas en inglés.

## *7.2 Estructura de los Subsistemas de Seguridad de la Información*

Cada uno de los Subsistemas de Seguridad de la Información contiene una serie de requerimientos a cumplir basados en controles, protocolos, reglas, procesos, metodologías, guías y formas de organización del flujo de trabajo de la Seguridad. Para facilitar su comprensión por parte del lector, los requerimientos serán clasificados dentro de Áreas de Seguridad de la Información y consecuentemente dentro de Dominios de Seguridad de la Información y por último dentro de los subsistemas de Seguridad de la Información.

Las distintas Áreas y Dominios de SI agrupan y categorizan a los diversos requerimientos del MRU de la siguiente forma:

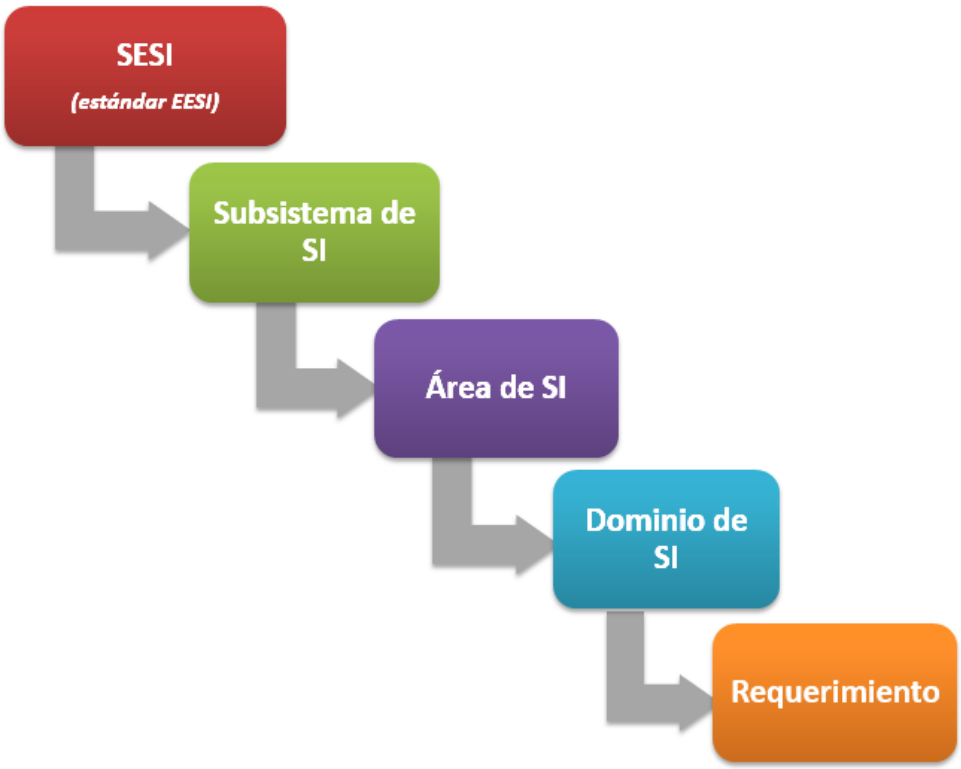



**Ilustración 7.2.1: clasificación y organización de requerimientos del MRU.**

A su vez, 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:

- Fundamentales (F): requerimientos obligatorios para declarar conformidad con un cierto nivel MRU.
- Claves (K): aquellos requerimientos necesarios para declarar conformidad con un cierto nivel intermedio[32] MRU.
- Especiales (S): a diferencia de la norma *ISO 27.001* [3], que plantea controles genéricos aplicables a cualquier tipo de organización[33], 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:
    a. Investigación y desarrollo.
    b. Contratistas de sectores sensibles de gobiernos.
    c. Sectores vinculados al resguardo de la composición, estructura y/o detalle de productos únicos y originales no patentados.
    d. Áreas vinculadas a los sectores de defensa y seguridad.
    e. Cualquier organización categorizada como una infraestructura crítica en función de la Directiva 2008/114/CE del Consejo de la Unión Europea [48].

  Dichas áreas críticas serán denominadas por el MRU como Áreas de Extrema Seguridad (AES).

## *7.3 Formato y estructura*

[32] 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 presente trabajo, para obtener mayor detalle sobre el presente tema.
[33] En función de lo establecido en la sección 1, página 8 de la Norma IRAM-ISO/IEC 27.001:2013 [2].

En función de lo establecido en la sección 3.1 del presente trabajo, el MRU se encontrará dividido en un primer nivel por los 11 SSI. Luego, se procederá a detallar cada una de las Áreas de SI correspondientes a dicho SSI, a su vez en cada de estas se detallarán todos los Dominios de SI abarcados por dicha Área. Cabe resaltar que dentro de cada Dominio de SI se describirán sus correspondientes requerimientos individuales.


**Ilustración 7.3.1: SSI, Áreas y Dominios de SI del MRU [27].**

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.

Los requerimientos se detallarán de la siguiente forma:

1. Como primer paso se detallará su código univoco, el estadio de madurez MRU al cual corresponde y su tipo (que podrá ser clave, fundamental o especial).
2. Luego, se procederá a detallar los procesos de los cuales forma parte dicho requerimiento.
3. En tercer lugar se incluirá la descripción del requerimiento en sí.
4. Luego, se detallarán los requerimientos MRU asociados a este.
5. Por último, se definirá la documentación fuente asociada a dicho requerimiento.

Se visualizará lo descripto anteriormente en la ilustración que se incluya a continuación.

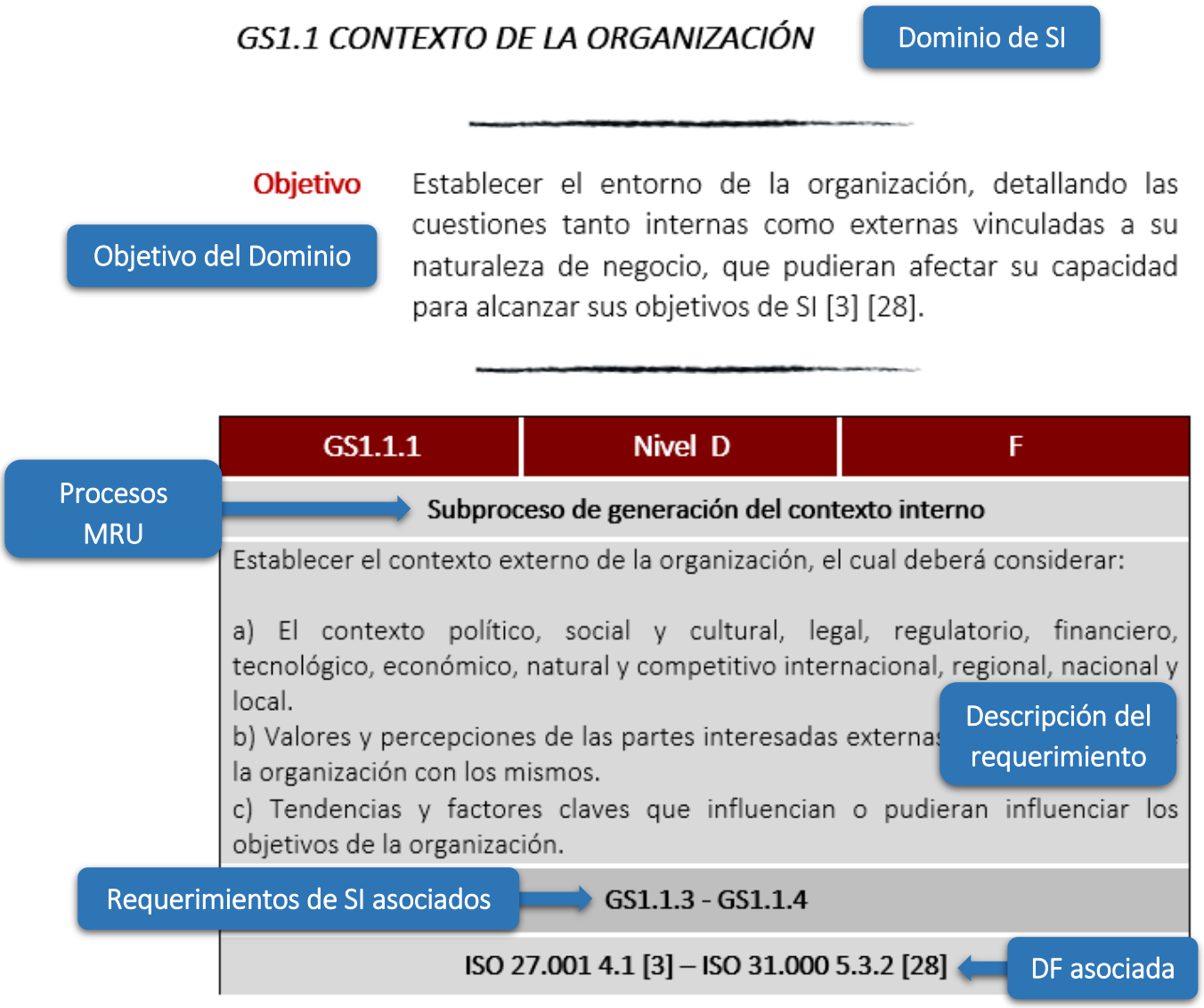



**Ilustración 7.3.2: ejemplo modelo de un Dominio de SI.**

Se incluye a continuación el modelo de un requerimiento individual del MRU:

| [Código univoco] | [Nivel MRU] | [Tipo de requerimiento] |
|---|---|---|
| [Proceso MRU] | | |
| [Descripción del Requerimiento] | | |
| [Requerimientos MRU asociados] | | |
| [DF asociada] | | |

**Ilustración 7.3.3: ejemplo modelo de un requerimiento del MRU.**

## *7.4 Subsistemas de Seguridad de la Información de ejemplo*

Se incluye a continuación los Subsistemas "*Gobierno de Seguridad de la Información*" y "*Lineamientos de Seguridad*" a modo de ejemplo, con el objetivo que el lector comprenda la magnitud y complejidad que se pretende alcanzar. Dichos Subsistemas forman parte del Sistema de Mejora Continua en Seguridad de la Información, que el MRU pretende desarrollar.

# GOBIERNO DE SEGURIDAD

El objetivo primordial del presente subsistema comprende el diseño, establecimiento, mantenimiento y monitoreo del Gobierno de Seguridad de la Información de la organización [41] [12].

Se enfoca principalmente en la creación de un Marco de Referencia de gobierno de SI a medida para la organización, en el armado de la estrategia de SI, en el alineamiento de esta última con los objetivos estratégicos del negocio y en la definición de las autoridades estratégicas de SI y sus correspondientes responsabilidades [41] [12] [4] [37].

## GOB1 Enfoque de gobierno de Seguridad de la Información [41] [12] [4]

*GOB1.1 Marco de Referencia de gobierno de SI*

*GOB1.2 Principios de gobierno de SI*

*GOB1.3 Macroprocesos de gobierno de SI*

*GOB1.4 Dirección estratégica de la seguridad de la información [37]*

## GOB2 Componentes del gobierno de SI [41] [12]

*GOB2.1 Estrategia de seguridad de la información*

*GOB2.2 Distribución de valor para las partes interesadas*

*GOB2.3 Sistema de Mejora continua de Seguridad de la Información*

# GOB1 ENFOQUE DE GOBIERNO DE SI

## *GOB1.1 Marco de Referencia de gobierno de SI*

**Objetivo** Lograr que el enfoque global de SI de la organización se encuentre respaldado por un Gobierno de SI en función de las directivas establecidas por COBIT, ISO, OCDE e ISF [41].

| GOB1.1.1 | Nivel C | F |
|---|---|---|
| **Proceso de diseño y creación del Marco de Referencia de gobierno de SI** | | |
| El órgano rector de gobierno de la organización (consejo de directores o equivalente) debe diseñar, establecer, dirigir, monitorear y comunicar un Marco de Referencia[34] de gobierno de Seguridad de la Información que:<br><br>a) Se encuentre basado en los principios establecidos en el Dominio de SI GOB1.2.<br>b) Implemente los Macroprocesos detallados en el Dominio de SI GOB1.3.<br>c) Incorpore las autoridades estratégicas de SI delineadas en GOB1.4.<br>d) Lleve adelante e implemente sus componentes descriptos en GOB2.<br>e) Deberá ser diseñado, establecido, dirigido, monitoreado y comunicado en función de un enfoque de gestión de riesgos que cuente con un sistema de control interno.<br><br>El órgano rector de gobierno de la organización tiene la responsabilidad final sobre la SI de la organización, no obstante puede de delegar los procesos y actividades de SI a un alto miembro de la dirección ejecutiva (el CISO). | | |

[34] "*Framework*" o marco de referencia en español.

El órgano rector de gobierno de la organización debe apoyar la SI a través de una dirección clara y concisa, mostrando y alentando el compromiso y estableciendo roles y responsabilidades de SI en la organización.

*El MRU establece requerimientos generales y estratégicos para el gobierno de SI (a través de los principios detallados en GOB1.2, los procesos establecidos en GOB1.3 y las autoridades estratégicas delineadas en GOB1.4 que centralizan las directivas de ISO, COBIT, OCDE y ISF para el gobierno de SI) con el objetivo de que cada organización tenga la libertad para diseñar su propio Marco de referencia de Gobierno de SI apropiado a su propia naturaleza, cultura y necesidades.*

*El órgano rector de gobierno[35] difiere de la dirección ejecutiva de la compañía[36]. El órgano rector se encuentra a cargo del gobierno de la organización y de sus actividades estratégicas, mientras que la dirección ejecutiva es responsable del gerenciamiento de la organización (aquí podemos encontrar las unidades de negocio o áreas de soporte tales como sistemas, Seguridad de la Información, RRRH, entre otras).*

GOB1.2 – GOB1.3 – GOB1.4 – GOB2

ISF Standard SG1 y SG2 [41] – ISO 27.014 4.2, 4.3, 5.2 y 5.3 [12] –
– COBIT II 4.3 [22] –

[35] Favor de referirse a la sección 0.5 del presente trabajo para una definición sobre el término utilizado.
[36] Favor de referirse a la sección 0.5 del presente trabajo para una definición sobre el término utilizado.

| GOB1.1.2 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI | | |
| El órgano rector de gobierno de la organización debe:<br><br>a) Internalizar la importancia de la Seguridad de la Información como un factor clave de éxito para el negocio.<br>b) Nombrar a un miembro del órgano rector de gobierno de la organización como responsable del Marco de referencia de gobierno de SI.<br>c) Asegurarse de que la estrategia de SI y el SMCSI de la organización apoyen y se encuentren alineados al Marco de Referencia de gobierno de SI establecido según el requerimiento GOB1.1.1.<br><br>El miembro del consejo de directores mencionado en b) será responsable por la aplicación del requerimiento GOB1.1.1. | | |
| GOB1.1.1 | | |
| ISF Standard SG1.1.2 [41] - ISO 27.014 4.2 y 4.3 [12] – ISO 27.001 5.1 [3] | | |

| GOB1.1.3 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br><br>Subproceso de establecimiento del Marco de Referencia | | |
| El órgano rector de gobierno de la organización debe demostrar su compromiso a través de la firma de:<br><br>a) El enfoque global de gobierno de SI tomado por la organización.<br>b) La estrategia de SI.<br>c) El SMCSI de la organización[37].<br>d) La PSI.<br>e) La arquitectura de SI para la organización. | | |
| | | |
| ISF Standard SG1.1.3 [41] | | |

[37] Se refiere a la firma del documento que establece el SMCSI objetivo de la organización. Dicho documento puede de encontrarse incluido dentro de la PSI.

| GOB1.1.4 | Nivel B | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de diseño de objetivos del Marco de Referencia | | |
| El órgano rector de gobierno de la organización debe definir los objetivos del Marco de Referencia de gobierno de SI, entre los cuales se deberán de incluir:<br><br>a) El alineamiento de la estrategia de SI, los objetivos de SI y el SMCSI de la organización con la estrategia y los objetivos del negocio y, a su vez, con la estrategia y los objetivos de TI.<br>b) La satisfacción de las necesidades de y la distribución de valor a las partes interesadas y al órgano rector de gobierno de la organización (como por ejemplo: reducción de costos, mejora de la reputación, mejora en la eficacia de la gestión de riesgos, etc.) en función de lo establecido en GOB2.2.<br>c) Asegurar que los riesgos de Seguridad de la Información están siendo abordados adecuadamente[38] y, a su vez, que una autoridad de la organización (preferentemente el CISO) sea responsable por la gestión de riesgos de SI.<br>d) Asegurarse que el enfoque de SI llevado adelante por la organización sea eficiente y efectivo. | | |
| GOB2.2 | | |
| ISF Standard SG1.1.3 [41] - ISO 27.014 4.2 y 4.3 [12] | | |

[38] Adecuadamente realiza una referencia relativa a que los riesgos sean gestionados a un nivel residual aceptable por parte de la organización, en función del apetito de riesgo establecido por el órgano rector de gobierno.

| GOB1.1.5 | Nivel B | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI | | |
| El órgano rector de gobierno de la organización (consejo de directores o equivalente) debe diseñar, establecer, dirigir, monitorear y comunicar un Marco de Referencia[39] de gobierno de Seguridad de la Información que:<br><br>a) Sea diseñado, establecido, dirigido, monitoreado y comunicado en función de un enfoque de gestión de riesgos que cuente con un sistema de control interno.<br>b) Establezca una política general de transparencia de las prácticas y procedimientos de gestión del riesgo de SI de la organización. | | |
| | | |
| ISF Standard SG1 y SG2 [41] – Principios SI OCDE 3 [49] | | |

| GOB1.1.6 | Nivel A | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI | | |
| El órgano rector de gobierno de la organización (consejo de directores o equivalente) debe diseñar, establecer, dirigir, monitorear y comunicar un Marco de Referencia[40] de gobierno de Seguridad de la Información que:<br><br>a) Tome como punto de referencia e insumo a la estrategia nacional y regional en Ciberseguridad. | | |
| | | |
| Principios SI OCDE [49] | | |

[39] "*Framework*" o marco de referencia en español.
[40] "*Framework*" o marco de referencia en español.

## *GOB1.2 Principios de gobierno de SI*

**Objetivo** Establecer las bases y directivas para el diseño e implementación del Marco de Referencia de gobierno de SI, a medida de cada organización.

| GOB1.2.1 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Organización y Responsabilidades | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Coordinar todas las actividades de SI de la organización.<br>b) Asegurarse que dichas actividades mencionadas en a) sean integrales[41] e integradas[42] a la organización.<br>c) Coordinar de forma ágil y precisa las actividades relacionadas con la Seguridad de la Información, primordialmente aquellas vinculadas con la seguridad física y lógica.<br>d) Establecer la responsabilidad sobre SI en toda la gama de actividades de la organización. Se deberá integrar y especificar dicha responsabilidad a los roles de la organización, por ejemplo a través del establecimiento de RAIs, RGs y otras autoridades establecidas por el MRU (favor de referirse a LS2.2). Se debe de prestar especial atención al establecimiento de la responsabilidad en los vínculos con las partes interesadas externas, aquellas secciones percibidas como "*fronteras*" o "*limites*" de la organización, como por ejemplo la información almacenada por un proveedor de servicios de almacenamiento en la "*nube*". | | |

[41] Se refiere a que deben alcanzar a todo el global de la organización o limitado al alcance definido en LS1.1.4.
[42] Se refiere a que las actividades de SI deben tomar en cuanta al negocio e integrarse a éste.

| |
|---|
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.1 [12] – PSI ONTI [37] – |

| GOB1.2.2 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de gestión de riesgos | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Garantizar que las decisiones sobre SI se realicen en función del riesgo.<br>b) Garantizar la toma de decisiones ágiles sobre las actividades de SI.<br>c) Garantizar que las decisiones sobre SI reflejan el apetito de riesgos de la organización (establecido en el requerimiento GR1.1.3) y son completadas de manera oportuna (por ejemplo, en función de una fecha acordada).<br>d) El órgano rector de gobierno de la organización asegure los recursos apropiados para implementar una correcta gestión de riesgos.<br>e) Garantizar que el proceso de gestión de riesgos de SI sea ejecutado de forma sistemática y cíclica.<br>f) Asegurar que la innovación sea considerada como una parte integral de la reducción de riesgo de SI al nivel aceptable establecido por la organización. | | |
| GR1.1.3 | | |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.2 [12] – PSI ONTI [37] – Principios SI OCDE 5, 6 y 7 [49] – | | |

| GOB1.2.3 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Integración al Negocio | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Asegurarse que la SI y los requisitos del MRU se encuentren integrados a los procesos existentes y futuros de la organización.<br>b) Establecer una estrategia para incorporar las actividades de SI a los procesos de negocio de la organización en función de lo establecido en a). | | |

| |
|---|
| c) Asegurar el establecimiento de la PSI y los objetivos y estrategia de SI, en función de GOB1.3.3.<br><br>*Para la implementación de b) se recomienda la utilización del enfoque BPM basado en la gestión de procesos (referirse a GOB1.2.7).* |
| |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.3 [12] – ISO 27.001 5.1 [3] – |

| GOB1.2.4 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br><br>Subproceso de conformidad con requerimientos[43] | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Respaldar el cumplimiento de los requerimientos legales, regulatorios, estatuarios, contractuales y de mercado.<br>b) Asegurar que las políticas y prácticas de SI estén de acuerdo e incorporen todos los requerimientos pertinentes detallados en a).<br>c) Asegurar que las políticas y prácticas de SI estén de acuerdo e incorporen todos los requerimientos normativos internos de la organización.<br>d) Asegurar el cumplimiento de a), b) y c) a través de la contratación y realización de auditorías de seguridad independientes. | | |
| | | |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.4 [12] | | |

[43] Podría a su vez ser denominado como subproceso de *"compliance"*.

| GOB1.2.5 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Recursos Humanos | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Ser construido en base al comportamiento humano.<br>b) Establecer una cultura que incorpore el comportamiento de SI en todos los RRHH de la organización.<br>c) Abordar como prioridad la implementación de actividades de educación, capacitación y toma de conciencia de SI, en marco del PCED del MRU.<br>d) Que el órgano rector de gobierno de la organización requiera, promueva y apoye la coordinación de las actividades de las partes interesadas en pos de lograr un rumbo y dirección coherente para la SI de la organización. | | |
| | | |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.5 [12] | | |

| GOB1.2.6 | Nivel C | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Seguimiento y Control | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Asegurar que el enfoque establecido por la organización para proteger su información cumple con el propósito de apoyar a la organización y provee los niveles de SI acordados para satisfacer los requerimientos del negocio.<br>b) Asegurar que las medidas de SI de la organización sean apropiadas y proporcionales al riesgo de SI al cual se encuentran dirigidas. | | |
| | | |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.6 [12] –<br>- Principios SI OCDE 6 [49] – | | |

| GOB1.2.7 | Nivel C | K |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de gestión de procesos | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Asegurar la correcta y efectiva implementación del enfoque BPM en función de los requerimientos del SMCSI.<br>b) Comunicar a toda la organización una cultura de SI orientada a procesos.<br>c) Establecer las responsabilidades vinculadas a los procesos (detalladas a lo largo del subsistema PM). | | |
| | | |

| GOB1.2.8 | Nivel B | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Organización y Responsabilidades | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de establecer los principios de SI de la organización. Dichos principios:<br><br>a) Serán desarrollados por el órgano rector de gobierno de la organización.<br>b) Serán comunicados a toda la organización.<br>c) Se encontrarán claramente documentados.<br>d) Deben ser limitados en número.<br>e) Estar expresados en un lenguaje simple.<br>f) Deben enunciar, tan claro como sea posible, los valores fundamentales de la organización.<br><br>Se deberán de incluir los siguientes principios desarrollados en forma conjunta por COBIT, ISF e $(ISC)^2$:<br><br>a) Fomentar una cultura positiva de SI.<br>b) Adoptar una estrategia basada en el riesgo para asegurar que el riesgo se trata de forma de forma consistente y efectiva.<br>c) Promover la mejora continua en SI.<br>d) Dar calidad y valor a las partes interesadas.<br>e) Centrarse e integrarse al negocio. | | |

| |
|---|
| *El presente requerimiento se encuentra estrechamente vinculado con GOB1.2.10.c.* |
| GOB1.2.10.c |
| COBIT II 2.2 [22] |

| GOB1.2.9 | Nivel B | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Seguimiento y Control | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Permitir al órgano rector de gobierno de la organización la visibilidad del estado de SI de la organización.<br>b) Medir el éxito del Marco de Referencia de gobierno de SI en términos de contribución a los objetivos de la organización.<br>c) Permitir al órgano rector de gobierno de la organización la evaluación la performance de SI en la organización en función de su impacto en el negocio (no se debe de hacer foco únicamente en la efectividad y eficiencia de los controles de seguridad). | | |
| | | |
| ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] | | |

| GOB1.2.10 | Nivel B | F |
|---|---|---|
| Proceso de diseño y creación del Marco de Referencia de gobierno de SI<br>Subproceso de Integración al Negocio | | |
| El Marco de Referencia de gobierno de SI deberá abordar la necesidad de:<br><br>a) Establecer una estrategia de inversión en SI basada en los resultados del negocio que permita la toma de decisiones sobre inversión en SI sean eficientes, efectivas y reflejen los objetivos del negocio.<br>b) Establecer una estrategia para incorporar las actividades de SI a los procesos de negocio de la organización en función de lo establecido en a). | | |

c) Asegurar que todos las partes interesadas comprendan los riesgos de SI y conozcan cómo gestionarlos (GOB1.2.2 establece mayor detalle sobre este aspecto).

*Para la implementación de b) se recomienda la utilización del enfoque BPM basado en la gestión de procesos (referirse a GOB1.2.11).*

*En función de c), las partes interesadas deberán de contar con la capacitación y las habilidades necesarias para comprender y gestionar los riesgos de SI y, a su vez, para evaluar el impacto potencial que sus decisiones de gestión de riesgos de SI tendrán sobre sus actividades y la organización.*

ISF Standard SG1.1.4, SG1.1.5 y SG1.1.6 [41] – ISO 27.014 5.2.3 [12] – Principios SI OCDE 1 [49] –

| GOB1.2.11 | Nivel A | F |
|---|---|---|

Proceso de diseño y creación del Marco de Referencia de gobierno de SI

Subproceso de Organización y Responsabilidades

El Marco de Referencia de gobierno de SI deberá abordar la necesidad de que todas las partes interesadas en función de sus roles, contexto y su capacidad de acción:

a) Implementen los principios y lineamientos del Marco de Referencia de gobierno de SI dentro de sus procesos de toma de decisiones.
b) Sean responsables por la gestión de los riesgos de SI.
c) Gestionen los riesgos de SI en una forma transparente, ética y coherente con los derechos humanos y los valores fundamentales.
d) Cooperen para lograr una eficiente y efectiva gestión de los riesgos de SI de la organización.

*El presente requerimiento se encuentra estrechamente vinculado con GOB1.2.10.c.*

GOB1.2.10.c

Principios SI OCDE 2, 3 y 4 [49]

[Página dejada en blanco intencionalmente]

## *GOB1.3 Macroprocesos de gobierno de SI*

**Objetivo** Establecer los Macroprocesos fundamentales que un Marco de Referencia de gobierno de SI eficiente y efectivo deberá de integrar y ejecutar [12] [41].

| GOB1.3.1 | Nivel C | F |
|---|---|---|
| Macroproceso de Gobierno de Seguridad de la Información | | |
| El Marco de Referencia de gobierno de SI deberá de comprender los siguientes macroprocesos:<br><br>a) Evaluar.<br>b) Dirigir.<br>c) Monitorear.<br>d) Comunicar.<br>e) Asegurar.<br><br>El órgano de gobierno de la organización será responsable por la ejecución de los macroprocesos a), b), c) y d). El objetivo del macroproceso e) consiste en proveer una opinión independiente y objetiva sobre el estado del gobierno de SI y el nivel de SI de la organización.<br><br>*Se incluye el diagrama ilustrativo de la norma ISO 27.014 (Figura 2 de dicha DF) [12] con el objetivo de facilitar la comprensión del presente requerimiento:* | | |

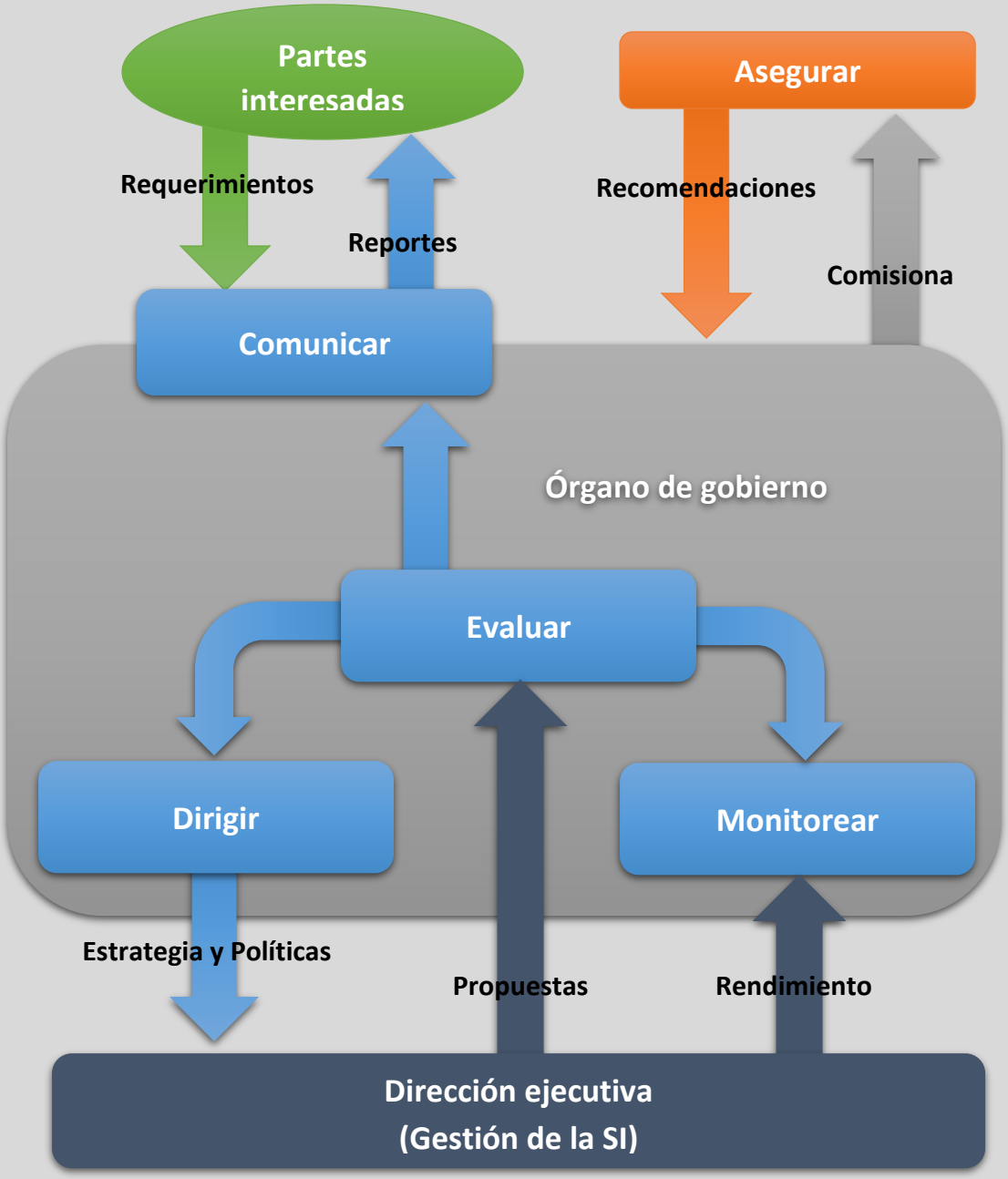



Ilustración GOB1.3.1.A: Macroprocesos de gobierno de SI [12].

*Vale la pena detallar las aclaraciones de la sección 4.4 de la norma ISO 27.014 [12], en la que se establece que cada modelo de gobierno especifico (tanto sea de SI o de TI, por ejemplo) conforma un componente integral del gobierno corporativo de la organización. Por este motivo, los alcances de los distintos modelos pueden llegar a superponerse. Este es el caso que se presenta entre los modelos de*

*gobierno de SI y de TI que puede observarse en la siguiente ilustración extraída de la norma previamente comentada:*

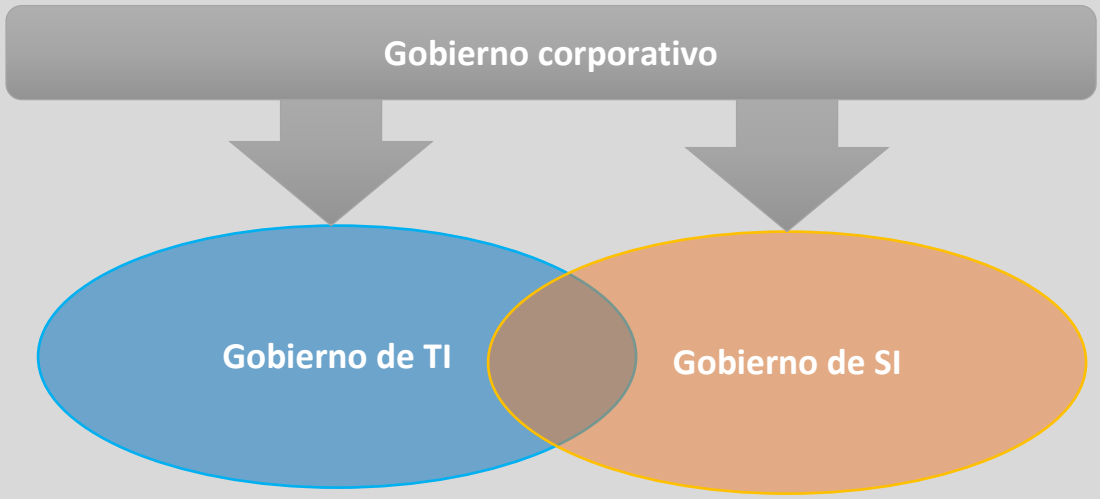



Ilustración GOB1.3.1.B: Superposición de los gobiernos de TI y SI [12].

ISO 27.014 5.3.1 [12]

| GOB1.3.2 | Nivel C | F |
|---|---|---|

Macroproceso Evaluar

El macroproceso GOB1.3.1.a (*Evaluar*) toma en cuenta el logro actual y estimado de los objetivos de SI basados en los cambios implementados y planeados y, determina si se requieren realizar ajustes para el logro de dichos objetivos en el futuro.

Dentro de dicho macroproceso, el órgano de gobierno de la organización debe:

a) Asegurar que las iniciativas del negocio consideran aspectos de SI.
b) Responder a los resultados sobre el rendimiento de la SI e iniciar y priorizar las acciones de ajuste requeridas.
c) Evaluar, a intervalos planificados, el grado en que la estrategia de SI satisface las necesidades del negocio y responde en consecuencia, en función del requerimiento GOB1.1.4.a.

d) Evaluar estratégicamente, a intervalos planificados, el SMCSI de la organización para asegurar que continúa siendo pertinente, adecuado y eficaz, en función del requerimiento GOB1.3.6 (Subproceso de revisión del SMCSI).

Dentro de dicho macroproceso, la dirección ejecutiva debe:

e) Asegurar que la SI colabora con y apoya adecuadamente a los objetivos de la organización.
f) Evaluar el SMCSI de la organización para asegurar que continúa siendo pertinente, adecuado y eficaz, en función del requerimiento GOB1.3.6 (Subproceso de revisión del SMCSI).
g) Recomendar al órgano rector de gobierno de la organización nuevos proyectos de SI que generen un impacto significativo en el logro de los objetivos de SI y de la organización, en función del requerimiento GOB1.2.3.a.

| GOB1.2.3.a – GOB1.3.6 – GOB1.1.4.a – GOB1.3.1.a |
|---|
| ISO 27.014 5.3.2 [12] - ISF Standard SG1.1.3 [41] |

| GOB1.3.3 | Nivel C | F |
|---|---|---|

Macroproceso Dirigir

El macroproceso GOB1.3.1.b (*Dirigir*) permite al órgano de gobierno de la organización dirigir la estrategia y objetivos de SI. Dicho proceso puede establecer cambios en los recursos asignados a SI, en la priorización de actividades de SI y en la aprobación de las políticas de seguridad y la actual gestión de riesgos.

Dentro de dicho macroproceso, el órgano de gobierno de la organización debe:

a) Dirigir la actividad de SI, determinando el apetito de riesgo de la organización (referirse al requerimiento GR1.1.3), respaldando la estrategia de SI y la PSI (refiriese al requerimiento GOB 2.1.1.e y a LS1.2.3.c) y determinando y proporcionando los recursos necesarios, según lo establecido en c).
b) Aprobar la estrategia de SI y la PSI (en función de GOB2.1.1.e).
c) Asegurar la disponibilidad y asignar los recursos e inversiones apropiadas para la SI de la organización, dirigidos al diseño, establecimiento, implementación, mantenimiento y mejora continua del SMCSI, en función del requerimiento GOB1.2.3.a.
d) Promover una cultura positiva de SI en toda la organización.

e) Exigir, dirigir y apoyar a otros roles de la alta dirección de la organización en el cumplimiento de los requerimientos del SMCSI y en la colaboración durante su diseño, implementación, mantenimiento y mejora.

Dentro de dicho macroproceso, la dirección ejecutiva debe:

f) Desarrollar la estrategia de SI (en función de GOB2.1 y GOB1.4.3) y la PSI (en función de LS1.2).
g) Alinear los objetivos de SI con los objetivos del negocio.
h) Promover una cultura positiva de SI en toda la organización.
i) Determinar y proponer al órgano de gobierno los recursos e inversiones apropiadas para la SI de la organización como entrada de proceso a lo determinado en c) en función del requerimiento GOB2.2.3.
j) Exigir, dirigir y apoyar a otros roles de la dirección ejecutiva en el cumplimiento de los requerimientos del SMCSI y en la colaboración durante su diseño, implementación, mantenimiento y mejora.

*El apartado i) busca obtener el apoyo, guía y recursos para una efectiva y correcta implementación del SMCSI.*

GR1.1.3 – GOB2.1 – GOB1.4.3 – LS1.3 – GOB 2.1.1.e – LS1.2.3.c – GOB1.2.3.a – GOB2.2.3 – GOB1.2.1.b

ISO 27.014 5.3.3 [12] - ISF Standard SG1.1.3 [41] – ISO 27.001 5.1 y 7.1 [3]

| GOB1.3.4 | Nivel C | F |
|---|---|---|

Macroproceso Monitorear

El macroproceso GOB1.3.1.c (*Monitorear*) permite al órgano de gobierno de la organización evaluar el grado de cumplimiento de los objetivos estratégicos de SI de la organización.

Dentro de dicho macroproceso, el órgano de gobierno de la organización debe:

a) Evaluar la efectividad de las acciones de gestión de SI y monitorear el éxito de la gestión de SI, en concordancia con el requerimiento GOB1.2.6, para asegurar que el SMCSI logra los resultados previstos.
b) Asegurar la conformidad de la organización con los requerimientos internos y externos y evaluar el grado de cumplimiento general con los requerimientos vinculados a SI, en concordancia con GOB1.2.4.

c) Considerar el impacto sobre la gestión del riesgo de SI que podrían tener los cambios legales y regulatorios y, a su vez, los cambios en la naturaleza y operaciones del negocio y las implicaciones generales del mapa cambiante de amenazas de SI, en concordancia con el requerimiento GOB1.2.2.
d) Asegurar el cumplimiento de las Áreas de SI GOB1.2 (principios de Gobierno de SI) y GOB1.3 (Macroprocesos de Gobierno de SI).
e) Promoviendo, dirigiendo y exigiendo la mejora continua.

Dentro de dicho macroproceso, la dirección ejecutiva debe:

f) Seleccionar, diseñar e implementar métricas de rendimiento adecuadas desde una perspectiva del negocio.
g) Retroalimentar al órgano rector de gobierno de la organización sobre los resultados de rendimiento de la SI en función de lo delineado por este y los impactos que la SI provocaron al negocio.
h) Alertar al órgano rector de gobierno de la organización sobre nuevos desarrollos que afecten la SI y sobre los riesgos relativos a los activos de información de la organización.

| GOB1.2.2 – GOB1.2.4 – GOB1.2.6 – GOB1.2 – GOB1.3 – GOB1.3.1.c |
|---|
| ISO 27.014 5.3.4 [12] - ISF Standard SG1.1.3 [41] – ISO 27.001 5.1 [3] |

| GOB1.3.5 | Nivel C | F |
|---|---|---|
| Macroproceso Comunicar | | |

El macroproceso GOB1.3.1.d (*Comunicar*) conforma un proceso de gobierno bidireccional en donde el órgano rector de gobierno y las partes interesadas intercambian información sobre SI, en función de sus necesidades específicas.

Dentro de dicho macroproceso, el órgano de gobierno de la organización debe:

a) Comunicar el estado de las actividades estratégicas y de alto nivel de SI a las partes interesadas, en función del Dominio de SI GOB2.2.
b) Reportar a las partes interesadas externas que la organización posee un nivel de SI proporcional a la naturaleza del negocio, en función del Dominio de SI GOB2.2.
c) Notificar a la dirección ejecutiva sobre las revisiones y auditorias independientes de SI que hayan reportado problemas y requerido la toma de

acciones correctivas, especificando donde se requieren implementar dichas acciones.
d) Reconocer las obligaciones legales, reglamentarias, contractuales, estatutarias y de mercado, las expectativas de las partes interesadas y las necesidades del negocio vinculadas a la SI.
e) Monitorear y revisar periódicamente el apetito de riesgo de la organización.

Dentro de dicho macroproceso, la dirección ejecutiva debe:

f) Recomendar e informar al órgano de gobierno de la organización cualquier asunto que requiera de su atención y, probablemente, de su decisión.
g) Instruir a las partes interesadas sobre las acciones detalladas que deberán de realizarse en apoyo a las directivas y decisiones del órgano de gobierno de la organización. Dicha instrucción deberá promover y difundir la importancia de una gestión de SI eficaz y conforme a los requerimientos del MRU.

*Los anexos A y B de la norma ISO 27.014 [12] establecen distintos ejemplos sobre cómo llevar adelante la comunicación con las partes interesadas, que podrían colaborar y simplificar la implementación del presente requerimiento. A su vez se deberá de tener en cuenta lo delineado en el Dominio GOB2.2.*

*El presente requerimiento es considerado fundamental para cualquier implementación, tanto parcial como completa del SMCSI: la comunicación de la importancia de SI y la implementación de un programa holístico de toma de conciencia, entrenamiento y difusión de la SI.*

| GOB2.2 – GOB1.3.1.d |
|---|
| ISO 27.014 5.3.5 [12] - ISF Standard SG1.1.3 [41] – ISO 27.001 5.1 [3] |

| GOB1.3.6 | Nivel C | F |
|---|---|---|
| Subproceso de Revisión del SMCSI | | |
| La revisión del SMCSI deberá de incluir consideraciones sobre:<br><br>a) El estado de las acciones tomadas en función de revisiones previas.<br>b) Los cambios internos y externos pertinentes al SMCSI y a la SI de la organización.<br>c) La retroalimentación de las partes interesadas. | | |

| |
|---|
| d) Los resultados de la evaluación del riesgo y el estado del plan de tratamiento del riesgo.<br>e) Las oportunidades de mejora continua.<br>f) La retroalimentación sobre el desempeño de la SI (deberá de incluir los resultados de auditoria, las no conformidades y sus acciones correctivas, los resultados del seguimiento y mediciones de SI y el logro de los objetivos de SI).<br><br>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.<br><br>Se deberá de conservar información documentada como evidencia de la ejecución del presente subproceso. |
| |
| ISO 27.001 9.3 [12] |

| GOB1.3.7 | Nivel B | F |
|---|---|---|
| Macroproceso Asegurar | | |
| El macroproceso GOB1.3.1.e (*Asegurar*) conforma a aquel por el cual el órgano rector de gobierno de la organización comisiona la realización de auditorías o revisiones independientes y objetivas e incluso certificaciones de ciertas normas o estándares de SI.<br><br>Dentro de dicho macroproceso, el órgano de gobierno de la organización debe comisionar la emisión de opiniones independientes y objetivas sobre cómo está cumpliendo los requerimientos del SMCSI de la organización, en cuanto a su responsabilidad.<br><br>Dentro de dicho macroproceso, la dirección ejecutiva debe apoyar y colaborar en su ejecución durante todo el proceso a dichas auditorias o revisiones independientes. | | |
| GOB1.3.1.e | | |
| ISO 27.014 5.3.6 [12] - ISF Standard SG1.1.3 [41] | | |

## *GOB1.4 Dirección estratégica de la SI*

**Objetivo** Establecer las autoridades estratégicas de SI y sus correspondientes responsabilidades dentro de la dirección ejecutiva de la organización [41] [12].

| GOB1.4.1 | Nivel E | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |
| La organización deberá de contar con un responsable de SI. | | |
| | | |
| | | |

| GOB1.4.2 | Nivel D | K |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |
| Se deberá contar con un CISO de tiempo completo nombrado dentro de la alta dirección ejecutiva de la organización, el cual será responsable por la implementación, la gestión, el mantenimiento, la supervisión y la mejora continua del SMCSI de la organización.<br><br>El CISO deberá de contar con la responsabilidad y los recursos necesarios para llevar adelante el presente requerimiento.<br><br>*Se deberá de denominar al responsable detallado en GOB1.4.1 como CISO.* | | |
| | | |
| ISF Standard SG1.2.1 y SM2.1.1 [41] – ISO 27.001 5.3 [3] | | |

| GOB1.4.3 | Nivel D | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |
| El CISO deberá:<br><br>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 tratamiento del riesgo de SI). El CSI será responsable por la implementación de la gestión de riesgos y por la aceptación de los niveles residuales de riesgos en función del apetito de riesgo definido por el órgano de gobierno de la organización (referirse a GR1.1.3).<br>b) Enfocarse en priorizar la protección de los procesos y aplicaciones críticas del negocio y, a su vez, la información sensible de la organización de filtraciones, modificaciones y accesos no autorizados.<br>c) Asegurar que el SMCSI de la organización se encuentra en conformidad con todos los requerimientos del MRU correspondientes al nivel respectivo implementado. A su vez, deberá de diseñar, obtener la aprobación e implementar las acciones correctivas y verificarlas en función del SSI SC. | | |

d) Desarrollar y documentar la misión y visión del área de SI de la organización, sobre la cual se basará el desarrollo de la estrategia de SI. Deberá de mantenerlas en el tiempo.
e) El CISO será responsable de desarrollar, buscar la aprobación, implementar y gestionar el SMCSI de la organización.
f) Informar sobre el rendimiento del SMCSI al CSI y a la alta dirección.
g) Coordinar y supervisar la SI en toda la organización.

*El órgano rector de gobierno será responsable por comunicar y asegurar que todos dentro de la organización colaboren en la concreción de a).*

| GR1.1.3 |
|---|
| ISF Standard SG1.2.2 y SM 2.1.1 [41] – [31] – ISO 27.001 [3] – [40] – ISO 27.002 6.1.1 [7] – [4] – PSI ONTI [37] – |

| GOB1.4.4 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |

El CISO deberá:

a) Desarrollar, implementar, comunicar y mantener una estrategia de SI y una PSI alineada al Marco de Referencia de gobierno de SI de la organización (favor de referirse al Dominio de SI GOB1.1).
b) Desarrollar y establecer el PESI en función de la estrategia de SI (debe de recordarse que la misma debe ser aprobada por el CSI y el órgano rector de gobierno de la organización según los requerimientos GOB1.3.3 y GOB1.4.6) en función del requerimiento GOB2.1.4.
c) Desarrollar, implementar, mantener y mejorar una arquitectura de SI (la cual deberá de contener la PSI, el SMCSI del organización, la estrategia de SI y el Marco de procesos[44] de SI) que provea un marco de referencia para el desarrollo, implementación, mantenimiento y mejora de controles estándar de Seguridad de la Información en toda la organización. La arquitectura de SI será diseñada acorde a cada organización.
d) Proporcionar formas de mejorar la eficiencia y la eficacia de la función de SI.
e) Definir y documentar los requerimientos de SI de la organización.

[44] Dentro del Subsistema PM, se establecerán los lineamientos para el desarrollo del Marco de Referencia a seguir para que el diseño de todos los procesos de la organización tengan en cuenta la SI.

f) Generar el presupuesto de la organización relativo a SI y supervisar y gestionar los fondos relativos a todas las tareas y actividades de SI de la organización.
g) Gestionar la mejora continua y el mantenimiento del SMCSI.
h) Ser responsable del diseño, desarrollo, gestión, mantenimiento y mejora continua de los procesos de SI.
i) Identificar y comunicar amenazas para la SI, comportamientos deseables y cambios necesarios para tratar estos puntos. A su vez debe de asegurar que se evalúe el impacto potencial de los cambios.

El CISO rendirá cuentas al órgano rector de gobierno de la organización directamente o a través del CEO.

*En cuanto a la implementación de i) se debe tener en cuenta que los requerimientos de SI de la organización son conformados por: requerimientos legales, reglamentarios, contractuales, estatutarios, del negocio y del mercado, objetivos estratégicos dela organización, riesgos de SI y necesidades de protección de SI de la organización.*

| GOB1.1 – GOB1.3.3 – GOB1.4.6 – GOB2.1.4 |
|---|
| ISF Standard SG1.2.2 [41] – [31] – ISO 27.001 [3] – [40] – [4] – ISO 27.002 6.1.1 [7] – COBIT C.1 [22] – PSI ONTI [37] – |

| GOB1.4.5 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br><br>Subproceso de establecimiento del CSI | | |
| Se deberá establecer un CSI (Comité de Seguridad de la Información) dentro de la organización. El Comité deberá estar integrado al menos por:<br><br>a) El CISO de la organización.<br>b) El RT (responsable/gerente del área de TI, tecnología o equivalente).<br>c) Representantes seleccionados por los responsables máximos de las áreas de soporte de la organización (RRHH, legales, PMO, riesgos, entre otros).<br>d) El CEO o un representante seleccionado por el mismo.<br>e) Uno o más responsables de las unidades de negocio de la organización.<br>f) Un miembro del órgano rector de gobierno de la organización o un representante del mismo, que ocupará el cargo de presidente del CSI. El presidente del CSI se encargará de coordinar todas las actividades del mismo. | | |

g) Un representante seleccionado por el responsable máximo del área de auditoria interna de la organización.
h) Los RAI responsables por aquellos procesos y aplicaciones de la organización considerados críticos.
i) CIPO y RMO.

*Es altamente probable que aquellos mencionados en c) se unan al CSI cuando sea relevante, a requerimiento del mismo, o sean considerados como miembros permanentes. Esto último, queda librado a discreción de cada organización.*

*Las organizaciones tendrán libertad para realizar la selección de los integrantes detallados en e) en función de sus necesidades y naturaleza particular.*

*Los integrantes mencionados en h) serán responsables de comunicar tanto iniciativas de negocio que puedan impactar en la SI como el impacto que las prácticas de SI puedan causar a los usuarios.*

ISF Standard SG1.2.4 y SG1.2.5 [41] – PSI ONTI [37] – [31] – [40]

| GOB1.4.6 | Nivel C | F |
|---|---|---|

Macroproceso de dirección estratégica de la SI

Subproceso de establecimiento del CSI

El CSI será responsable de brindar apoyo y asegurar la colaboración de todas las áreas de la organización para el desarrollo, implementación, mantenimiento, verificación de conformidad y mejora continua del SMCSI por parte del CISO.

El CSI debe:

a) Reunirse regularmente.
b) Coordinar las actividades estratégicas de SI en toda la organización.
c) Revisar regularmente, aprobar y establecer la estrategia y los objetivos de SI y la PSI. A su vez debe de asegurar la compatibilidad de la estrategia y objetivos de SI con los objetivos de negocio de la organización.
d) Promover la mejora continua de la SI en toda la organización.
e) Asegurarse que la SI se encuentra integrada dentro de la metodología desarrollo de software de la organización.

f) Aprobar las políticas de SI (los procesos, normas, guías y procedimientos resultantes de la "bajada a tierra" de las políticas de SI serán analizados y aprobados por el CEP).
g) Monitorear y supervisar el rendimiento de la SI de la organización. A su vez, evaluará y coordinará la implementación de controles de SI y su correspondiente planeación, factibilidad y diseño.
h) Revisar, aprobar y establecer la arquitectura de SI de la organización (en función del requerimiento GOB1.4.3).
i) Revisar regularmente la estrategia de SI con el objetivo de asegurarse que continúa alineada a los objetivos de la organización y que continúa ofreciendo el retorno de inversión planeado.
j) En función de la revisión continua detallada en n), el CSI deberá analizar y aprobar cambios a la estrategia de SI.
k) Aceptar y aprobar el nivel de riesgo residual resultante de la gestión de riesgos de SI efectuada por el EGR, en función del apetito de riesgos de la organización (referirse a GR1.1.3). Por lo que, deberá de supervisar la gestión de riesgos de SI de la organización.
l) Revisar en forma periódica que el SMCSI de la organización se adecua a sus necesidades y sus requerimientos (en función de GOB1.4.4). A su vez, deberá de asegurarse que las prácticas de SI se apliquen eficazmente y consistentemente a lo largo de la organización.
m) Difundir la SI y apoyar el desarrollo del PCED de la organización.
n) Supervisar la gestión, mantenimiento y mejora continua de los procesos de SI.
o) Supervisar el monitoreo, análisis e investigación de incidentes de SI.
p) Supervisar la gestión de la continuidad del negocio y la implementación de los controles de SI.
q) Identificar a los RAI y RGs.
r) Identificar como gestionar las no conformidades.

*El CSI será responsable de aprobar las decisiones clave que afecten el estado de SI de la organización, por lo que su conformación y metodología de trabajo impactaran significativamente en el nivel de SI que podrá alcanzar la organización.*

GOB1.4.3 – GOB1.4.5 – GR1.1.3 – GOB1.4.4

ISF Standard SG1.2.4, SG1.2.6, SG1.2.7 y SG2.1.11 [41]– [31] – ISO 27.001 5.2, 5.3, 6.2 y 8.3 [3] – ISO 27.002 6.1.1 [7] – [4]

| GOB1.4.7 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CSI | | |
| La organización deberá de establecer el mecanismo por el cual el CSI aprobará sus decisiones.<br><br>*Se recomienda que el mecanismo de aprobación se base en el voto positivo de la mayoría calificada de sus miembros. Otra posibilidad que se podrá barajar consiste en dotar al presidente del CSI y/o al miembro detallado en GOB1.4.5.d de la facultad de veto de todas las acciones del CSI y, de esta forma requerir únicamente la mayoría absoluta de los miembros del Comité de SI.* | | |

| GOB1.4.8 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento de objetivos de SI | | |
| Los objetivos estratégicos de SI, que deben ser establecidos por el CSI (referirse a GOB1.4.6.c), serán utilizados como base para delinear los objetivos de SI de menor nivel (tanto tácticos como estratégicos) a funciones y niveles pertinentes.<br><br>Los objetivos de SI deben:<br><br>a) Ser compatibles con la estrategia y los objetivos de negocio de la organización.<br>b) Ser coherentes con la PSI de la organización.<br>c) Ser medibles (de ser posible).<br>d) Ser comunicados a toda la organización.<br>e) Ser actualizados periódicamente.<br>f) Tener en cuenta los requerimientos de SI pertinentes y los resultados de la evaluación y tratamiento del riesgo.<br>g) Ser acordes y desprenderse con un menor nivel de abstracción de los objetivos delineados en el requerimiento GOB1.1.4.<br><br>Los objetivos de SI deberán de estar correctamente documentados (dentro de la PSI de la organización) en función del requerimiento LS1.2.3.f. | | |

| |
|---|
| GOB1.1.4 – LS1.2.3.f – GOB1.4.6.c |
| ISO 27.001 6.2 [3] |

| GOB1.4.9 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento de objetivos de SI | | |
| Al planificar como lograr sus objetivos de SI, la organización deberá determinar:<br><br>a) Que es lo que se va a hacer.<br>b) Que recursos se van a necesitar.<br>c) El responsable de dicha implementación.<br>d) Tiempos estimados de logro.<br>e) Forma de medición y evaluación de los resultados.<br><br>Todos los apartados anteriores deberán basarse en el plan que deberá ser implementado por el CISO (PESI), en función de lo establecido en GOB2.1.4. | | |
| GOB2.1.4 | | |
| ISO 27.001 8.1 [3] | | |

| GOB1.4.10 | Nivel B | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |
| El CISO deberá de contar con las siguientes habilidades:<br><br>a) Tener un entendimiento exacto de la visión estratégica del negocio.<br>b) Ser un comunicador efectivo.<br>c) Ser hábil en construir relaciones efectivas con los líderes del negocio.<br>d) Ser capaz de traducir los objetivos del negocio en requerimientos de SI.<br><br>*El CISO deberá de validar los requerimientos de SI con las partes interesadas.* | | |
| | | |
| ISF Standard SG1.2.2 [41] – [31] – ISO 27.001 [3] – [40] – COBIT C.1 [22] – [4] – | | |

| GOB1.4.11 | Nivel B | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CSI | | |
| El CSI debe:<br><br>a) Supervisar y analizar la inteligencia sobre amenazas de SI y realizar recomendaciones al órgano rector de gobierno de la organización de cómo responder a nuevas y cambiantes amenazas.<br>b) Promover que la toma de decisiones sobre riesgo de SI tenga en cuenta las nuevas amenazas emergentes a los activos de información de la organización.<br>c) Asegurarse que la SI conforma una de las consideraciones dentro de todos los procesos de planeamiento del negocio.<br>d) Supervisar la investigación y monitoreo de los incidentes de SI.<br>e) Monitorear cambios significativos en los riesgos asociados a AI.<br><br>*La implementación de a) requiere del monitoreo ante cambios significativos en el entorno y en la organización que puedan significar una mutación de riesgos/amenazas de SI.*<br><br>*En función de la implementación de a) se deberá de establecer un proceso de comunicación y toma de conocimiento de incidentes de SI por parte del CSI.* | | |
| | | |
| ISF Standard SG1.2.4, SG1.2.6, SG1.2.7 y SG2.1.11 [41] – [31]<br>– ISO 27.002 6.1.1 [7] – [4] – | | |

| GOB1.4.12 | Nivel A | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br>Subproceso de establecimiento del CISO | | |
| El CISO deberá adoptar un enfoque basado en el negocio para su gestión de la SI en la organización:<br><br>a) Estableciendo una relación con las comunidades técnicas y de negocio en toda la organización con el objetivo de promover el valor y la importancia de SI.<br>b) Diseñando y distribuyendo soluciones de seguridad que tomen en cuenta los RRHH, los procesos y la tecnología de la organización y se encuentren basadas en | | |

| |
|---|
| la gestión de riesgos, para que estas sean luego implementadas y gestionadas por áreas de negocio y de TI.<br>c) Desarrollando y gestionando el desarrollo profesional del personal de SI (en función de los requerimientos del SSI ON) con el objetivo de que sean capaces de diseñar y distribuir soluciones de seguridad alineadas al negocio. |
| |
| ISF Standard SG1.2.3 [41] – [4] |

| GOB1.4.13 | Nivel A | F |
|---|---|---|
| Macroproceso de dirección estratégica de la SI<br><br>Subproceso de establecimiento del CSI | | |
| El CSI debe:<br><br>a) Reportar a las partes interesadas sobre riesgos identificados, progresos de la SI dentro de la organización, proyectos e iniciativas de seguridad, entre otros.<br>b) Promover la resiliencia contra impactos potenciales significativos al negocio (como por ejemplo aquellos asociados a los ciberataques dirigidos). | | |
| | | |
| ISF Standard SG1.2.4, SG1.2.6, SG1.2.7 y SG2.1.11 [41]– [31] – ISO 27.002 6.1.1 [7] – [4] – | | |

# GOB2 COMPONENTES DEL GOBIERNO DE SI

## *GOB2.1 Estrategia de Seguridad de la Información*

**Objetivo** Establecer los principios fundamentales para el desarrollo de una estrategia de SI efectiva que colabore y contribuya al logro de los objetivos de la organización [41].

| GOB2.1.1 | Nivel C | K |
|---|---|---|
| **Proceso de diseño de la estrategia de SI** | | |
| El gobierno de seguridad de SI de la organización debe estar respaldado por una estrategia de SI. La misma deberá:<br><br>a) Encontrarse documentada (en el Plan Estratégico de SI o PESI).<br>b) Ser revisada regularmente.<br>c) Ser diseñada, desarrollada y mantenida por el CISO de la organización.<br>d) Ser aprobada y establecida por el CSI (referirse a GOB1.4.6)<br>e) Ser aprobada y firmada por el órgano rector de gobierno de la organización (referirse a GOB1.1.3).<br>f) Ser de alto nivel[45] y estar basada en principios.<br>g) Delinear como la SI se alineará a los objetivos del negocio.<br>h) Justificar la importancia de la SI y describir como el valor de la función de SI dentro de la organización se incrementará de forma continua con el correr del tiempo. | | |

[45] Recordemos que aquí nos manejamos a nivel estratégico con un alto nivel de abstracción.

i) Tomar en cuenta el contexto del negocio (detallado en los requerimientos LS1.1.1 y LS1.1.2) y el contexto actual de la SI en la organización (habilidades, capacidades, apreciación de la SI en la organización, cultura de seguridad, etc.).
j) Tomar en cuenta la misión y visión documentada del área de SI de la organización (especificada en GOB1.4.3.g).
k) Tomar en cuenta los objetivos estratégicos y de operación de la organización.
l) Tomar en cuenta los criterios de éxito que serán utilizados para demostrar el valor del área del SI y sus progresos en función de los objetivos de SI.
m) Ser ajustada en función de los cambios producidos en la estrategia del negocio, en el entorno de amenazas de seguridad y en los factores externos e internos (políticos, económicos, sociales, tecnológicos, legales, etc.).

GOB1.3.3 - GOB1.4.3 – GOB1.4.6 – GOB1.1.2 – GOB1.1.3 – LS1.1.1 – LS1.1.2

ISF Standard SG2.1.1, SG2.1.4, SG2.1.6 y SG2.1.9 [41] – [31]

| GOB2.1.2 | Nivel C | F |
|---|---|---|

Proceso de diseño de la estrategia de SI

Subproceso de alineamiento

La estrategia de SI deberá demostrar como colaborará en el logro de los objetivos de la organización, a través de la definición de:

a) Como proveerá el retorno de la inversión en SI.
b) Como las actividades de SI colaborarán en el establecimiento de la resiliencia contra incidentes de gran impacto (como por ejemplo ciberataques significativos de alto impacto) y asegurarán la continuidad de las operaciones del negocio.
c) Un enfoque balanceado que combine la gestión de riesgos de información (en función del apetito de riesgos de la organización) y el cumplimiento de todos los requerimientos legales, regulatorios, contractuales, estatutarios y de mercado.
d) La importancia de que la SI aborde los riesgos relativos al mercado, a la conformidad con regulaciones, leyes y contratos y a las cambiantes amenazas vinculadas al avance de la tecnología.
e) El rol que los proyectos individuales de SI jugarán al lograr la realización de iniciativas estratégicas específicas.
f) Como la SI agregará valor a la organización (por ejemplo reduciendo costos o mejorando la reputación) y protegerá los intereses de las partes interesadas.

ISF Standard SG2.1.2 [41]

| GOB2.1.3 | Nivel C | F |
|---|---|---|
| Proceso de diseño de la estrategia de SI<br><br>Subproceso de justificación de SI | | |
| La estrategia de SI deberá demostrar como colaborará a defender a la organización de amenazas a la seguridad, a través de la definición de:<br><br>a) Delineando la forma en que el SMCSI colaborará a la organización a mantener su dirección estratégica (por ejemplo, respondiendo a la continua evolución de las amenazas de seguridad que podrían desviar o detener la dirección estrategia de la organización).<br>b) Describiendo como los proyectos de SI protegerán a la organización de posibles impactos adversos al negocio vinculados a iniciativas específicas (por ejemplo, una nueva unidad de negocio basada en el comercio electrónico o el envío seguro de información a los clientes a través de internet).<br>c) Detallando y explicando como la gestión de incidentes de SI conformará un elemento clave de la estrategia de SI. | | |
| | | |
| ISF Standard SG2.1.3 [41] | | |

| GOB2.1.4 | Nivel C | F |
|---|---|---|
| Proceso de generación del PESI | | |
| La estrategia de SI deberá ser ejecutada a través del diseño y establecimiento del plan estratégico de SI (PESI). El cual deberá:<br><br>a) Ser utilizado para el desarrollo de diversos programas de SI en función del enfoque 3P (Plan-Programa-Proyecto), con el objetivo de "bajar a tierra" la estrategia de SI en proyectos individuales de menor nivel de abstracción que, ejecutados en conjunto colaborarán en el logro los objetivos de SI de la organización.<br>b) Ser utilizado para monitorear el progreso de SI y comunicarlo a las partes interesadas.<br>c) Ser diseñado por el CISO de la organización.<br>d) Plasmar la estrategia de SI en cumplimiento con GOB2.1.1 y GOB2.1.2.<br>e) Definir la situación actual de SI y el futuro deseado. | | |

f) Delinear de forma estratégica y en alto nivel un plan de implementación del PESI (el cual definirá los recursos propios y/o externos, tiempos y costos y la justificación económica de las iniciativas de SI).
g) Tomar en cuenta las necesidades de capacitación de RRHH y gestión del cambio para la implementación de la estrategia de SI.
h) Detallar su propósito y alcance.

*El PESI podrá descomponerse en múltiples programas de SI que impulsarán diversas acciones de seguridad tendientes a lograr uno o más de los objetivos de SI de la organización. A su vez, dichos programas podrán descomponerse en múltiples proyectos de SI que en su conjunto implementarán el programa del cual se desprenden. Dicha metodología de acción es llamada por el **MRU** como enfoque 3P (Plan-Programa-Proyecto). Dicho enfoque consiste en proceder a disminuir el nivel de abstracción de las acciones de SI con el objetivo de lograr implementarlas y de esta forma hacer realidad la estrategia de SI.*

GOB2.1.1 – GOB2.1.2

ISF Standard SG2.1.7 [41] – [31]

| GOB2.1.5 | Nivel C | F |
|---|---|---|

Proceso de revisión y monitoreo de la estrategia de SI

El CISO deberá monitorear la implementación y la efectividad de la estrategia de SI. Para lo cual deberá:

a) Obtener retroalimentación continua de las partes interesadas.
b) Medir el progreso en función de los objetivos para identificar posibles vulnerabilidades de seguridad y lecciones aprendidas que podrán ser tomados en cuenta para futuras iniciativas de SI.
c) Asegurarse que los objetivos estratégicos de SI – y por lo tanto la estrategia de SI – continúan siendo válidos.

ISF Standard SG2.1.8 [41]

| GOB2.1.6 | Nivel C | F |
|---|---|---|
| Proceso de comunicación de la estrategia de SI | | |
| Se deberá de comunicar el valor de la estrategia de SI a las partes interesadas. La misma deberá de incluir los *"quick wins"*[46] y estar basada en el propósito de crear una confianza sostenida en cuanto a SI por parte de la organización para las partes interesadas. | | |
| | | |
| ISF Standard SG2.1.10 [41] | | |

| GOB2.1.7 | Nivel B | F |
|---|---|---|
| Proceso de diseño de la estrategia de SI<br><br>Subproceso de alineamiento | | |
| La estrategia de SI deberá estar integrada con la estrategia de negocio y con la estrategia de TI. Para lograr esto, se deberá:<br><br>a) Involucrarse con las partes interesadas con el objetivo de obtener consenso sobre qué es lo que se requiere para el logro de los objetivos de negocio y el aseguramiento del éxito organizacional.<br>b) Anticiparse y planear potenciales cambios tanto internos como externos con el objetivo de asegurarse que la organización continúa en una posición estratégicamente ventajosa para sus operaciones.<br>c) Construir resiliencia a través de la estrategia de SI con el objetivo de colaborar a la organización a resistir impactos adversos de amenazas probables e inesperadas. | | |
| | | |
| ISF Standard SG2.1.5 [41] | | |

[46] Aquellos logros que son fáciles y rápidos de alcanzar pero que logran brindar un gran impacto positivo en la gestión de SI.

## *GOB2.2 Distribución de valor para las partes interesadas*

**Objetivo** Implementar procesos efectivos de distribución de valor a las partes interesadas. A su vez, hará hincapié en la medición de la efectividad de dichos procesos [41] [22].

| GOB2.2.1 | Nivel B | K |
|---|---|---|

**Proceso de distribución de valor de SI**

Se deberá de utilizar la metodología de "*cascada de metas*" planteada por COBIT, con el objetivo de moldear los distintos requerimientos del SMCSI de la organización al contexto propio de la misma. La aplicación de dicha metodología garantizará que los proyectos de SI se encuentren perfectamente alineados a las necesidades de las partes interesadas de la organización.

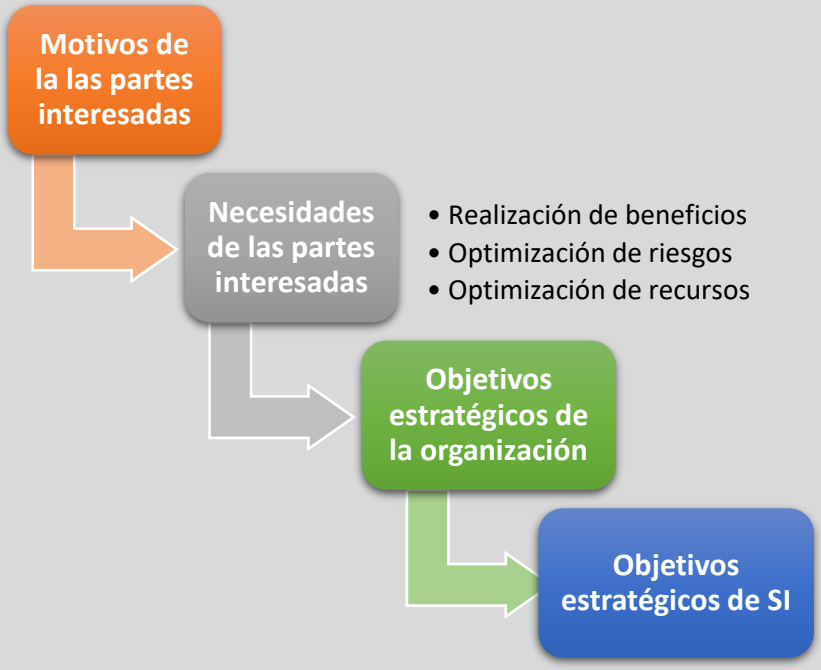



Ilustración GOB2.2.1.A: Visión general de la Cascada de Metas de COBIT 5 [22]

| |
|---|
| *En la cascada de metas, las necesidades de las partes interesadas (influenciadas por diversos motivos), se traducen y se concretan en los objetivos estratégicos de la organización. Para cumplir con dichos objetivos estratégicos, se requiere a su vez traducirlos a los objetivos vinculados a SI, y finalmente estos traducirlos en los correspondientes proyectos del área de SI de la organización (a través de la realización del PSI y los subsecuentes programas de SI que abarcarán dichos procesos).* |
| |
| COBIT Principio 1 [22] |

| GOB2.2.2 | Nivel B | F |
|---|---|---|
| Proceso de distribución de valor de SI | | |
| El valor distribuido a las partes interesadas por las iniciativas clave de SI deberá:<br><br>a) Optimizarse a través del cálculo de retorno de la inversión en seguridad (conocido generalmente como ROSI[47]) identificando los beneficios financieros o cuantitativos y los no-financieros o cualitativos.<br>b) Ser documentado de forma no técnica (debe de poder ser comprendido por aquellos no especializados en SI).<br>c) Ser reportado a la dirección ejecutiva y al órgano rector de gobierno de la organización. | | |
| | | |
| ISF Standard SG2.2.3 y SG2.2.4 [41] | | |

[47] Retorno de la inversión en seguridad, por sus siglas en inglés.

| GOB2.2.3 | Nivel B | F |
|---|---|---|
| Proceso de distribución de valor de SI | | |
| Las iniciativas de SI deberán contar con un plan de negocio[48] que:<br><br>a) Detalle claramente como la iniciativa contribuirá al logro de los objetivos del negocio y brindará valor a la estrategia de SI.<br>b) Incluya detalles sobre la necesidad de la incorporación de RRHH adicionales al equipo de SI de la información o sobre la necesidad de adquisición de productos/servicios de SI.<br>c) Sea firmado por un gerente del negocio.<br>d) Detalle una estimación sobre el retorno de la inversión esperado en función de beneficios cualitativos y cuantitativos.<br>e) Detalle como la iniciativa hará el mejor uso posible de los recursos de SI.<br>f) Explique porque los actuales recursos de SI son insuficientes.<br><br>El plan de negocio deberá estar sujeto a un proceso de escalamiento que se ejecutará cuando haya un:<br><br>g) Alineamiento insuficiente o ineficaz entre la iniciativa y los objetivos del negocio.<br>h) Uso insuficiente o ineficaz de los actuales recursos de SI. | | |
| | | |
| ISF Standard SG2.2.6, SG2.2.7 y SG2.2.8 [41] | | |

[48] También conocido generalmente como *"business case"*.

| GOB2.2.4 | Nivel B | F |
|---|---|---|
| Proceso de distribución de valor de SI | | |
| El órgano rector de gobierno de la organización deberá identificar y documentar los requerimientos de las partes interesadas con el objetivo de que el área de SI pueda establecer la dirección de su distribución de valor en función del cumplimiento de dichos requerimientos.<br><br>El órgano rector de gobierno deberá promover el papel primordial que toma la SI en la mejora de la agilidad de la organización.<br><br>*La SI juega un rol fundamental al permitir la difusión de barreras a la hora de la implementación de nuevos servicios o actividades clave de la organización (como por ejemplo, el uso de una infraestructura basada en AES-256 para la comunicación con organizaciones socias o la utilización de "nubes" de archivos de forma segura).* | | |
| | | |
| ISF Standard SG2.2.1 y SG2.2.2 [41] | | |

## *GOB2.3 Sistema de Mejora continua de SI: SMCSI*

**Objetivo** Establecer los fundamentos principales para el diseño del SMCSI a medida de cada organización.

| GOB2.3.1 | Nivel E | F |
|---|---|---|
| Proceso de diseño y desarrollo del SMCSI | | |
| El SMCSI de la organización deberá:<br><br>a) Tomar en cuenta las interdependencias entre los procesos de negocio de la organización y las partes interesadas tanto externas como internas.<br>b) Incluir un proceso de reporte anónimo para aquellos empleados que han tomado conocimiento de la comisión de alguna actividad ilícita o incidente de SI en la organización.<br>c) Determinar a un rol responsable por la SI de la organización (en concordancia con GOB1.4.1). | | |
| GOB1.4.1 | | |
| ISF Standard SG2.3.3, SG2.3.4, SG2.3.5 y SG2.3.6 [41] | | |

| GOB2.3.2 | Nivel D | F |
|---|---|---|
| Proceso de diseño y desarrollo del SMCSI | | |
| El SMCSI de la organización deberá:<br><br>a) Reflejar el apetito de riesgo de la organización.<br>b) Ser consistente con la gestión y el reporte de otros tipos de riesgos en la organización.<br>c) Asegurar que los requerimientos de SI sean identificados en función de una evaluación tanto de riesgos como de requerimientos legales, regulatorios, contractuales, estatutarios y de mercado.<br>d) Ser aplicado de forma consistente en toda la organización (el presente apartado podrá variar en función de lo determinado en LS1.1.4).<br>e) Ser gestionado por un CISO.<br>f) Brindar una noción general sobre la importancia de la SI a toda la organización (el presente apartado podrá variar en función de lo determinado en LS1.1.4).<br><br>El SMCSI deberá ser de aplicación obligatoria para todos los RRHH de la organización. Los mismos deberán de conocer, cumplir y hacer cumplir los diversos requerimientos del SMCSI de la organización. | | |
| LS1.1.4 | | |
| ISF Standard SG2.3.3, SG2.3.4, SG2.3.5 y SG2.3.6 [41] | | |

| GOB2.3.3 | Nivel C | F |
|---|---|---|
| Proceso de diseño y desarrollo del SMCSI | | |
| El SMCSI de la organización deberá:<br><br>a) Vincular el comportamiento esperado en cuanto a SI con las normas y valores de la organización.<br>b) Garantizar la implementación de un Marco de Referencia de gobierno de SI acorde al tamaño y naturaleza de la organización.<br>c) Asegurar el establecimiento del programa de toma de conciencia, entrenamiento y difusión de la SI.<br>d) Delinear dos enfoques de gestión de la SI: uno relativo al día a día y operaciones de SI y otro relativo al estado futuro y la mejora continua de la SI. | | |

*El SMCSI deberá ser de aplicación obligatoria para todas las partes interesadas internas de la organización (gerentes, propietarios y empleados) y, a su vez, para todos los usuarios de terceras partes de los AI de la organización y consultores o contratistas contratados por la misma. Los mismos deberán de conocer, cumplir y hacer cumplir los diversos requerimientos del SMCSI de la organización.*

ISF Standard SG2.3.3, SG2.3.4, SG2.3.5 y SG2.3.6 [41]

| GOB2.3.4 | Nivel B | F |
|---|---|---|

**Proceso de diseño y desarrollo del SMCSI**

El SMCSI de la organización deberá:

a) Asegurar el monitoreo de la eficiencia y eficacia de las actividades de SI a través del uso de técnicas cuantitativas y la comparación contra indicadores clave de rendimiento (conocidos generalmente como KPIs[49]).
b) Establecer el reporte de los resultados del monitoreo de SI detallado en a) al órgano rector de gobierno de la organización.
c) Contemplar un proceso de toma de medidas correctivas en función del análisis de los resultados del monitoreo de SI.
d) Establecer un marco de referencia de continuidad del negocio.
e) Establecer un área de diseño, implementación, gestión y mejora de los procesos de SI. Si la organización ya cuenta con un área de procesos, el área de procesos de SI podrá depender de esta.
f) Ser de aplicación obligatoria para los clientes, proveedores, socios y cualquier tipo de entidad vinculada a la organización. Por lo que, será de aplicación y cumplimiento obligatorio para todas las partes interesadas.

*La organización se encargará de delinear las formas de implementación y control de f). Se recomienda el establecimiento de PSIs específicas para cada parte interesada detallada en el presente requerimiento.*

*En el caso de proveedores, socios y clientes se recomienda el desarrollo e implementación de una PSI especifica entre la organización y la parte interesada correspondiente.*

ISF Standard SG2.3.3, SG2.3.4, SG2.3.5 y SG2.3.6 [41]

[49] *"Key Performance Indicators"* por sus siglas en inglés.

| GOB2.3.4 | Nivel A | F |
|---|---|---|
| Proceso de diseño y desarrollo del SMCSI | | |
| El SMCSI de la organización deberá:<br><br>a) Asegurar el establecimiento de una estructura natural en el área de SI de la organización.<br>b) Asegurar la ejecución de los procesos de SI a través de herramientas BPMS.<br>c) Implementar las medidas relativas a las AES.<br>d) Establecer un equipo de seguridad ofensiva según lo delineado en el SSI SC. | | |
| | | |
| ISF Standard SG2.3.3, SG2.3.4, SG2.3.5 y SG2.3.6 [41] | | |

[Página dejada en blanco intencionalmente]

# LINEAMIENTOS DE SEGURIDAD

El presente subsistema tiene como objetivo primordial el establecimiento de las bases principales de la mejora continua en Seguridad de la Información.

Se enfoca principalmente en el diseño y establecimiento de políticas y normas de uso, en las bases de la operatoria del día a día de la seguridad, en la gestión de proyectos de SI, en la consideración y análisis de los requerimientos legales y regulatorios y en la organización general de la Seguridad de la Información.

## LS1 Organización general de la Seguridad de la Información [37] [3] [7]

*LS1.1 Contexto de la organización & Implementación del SMCSI*

*LS1.2 Política de Seguridad de la Información*

*LS1.3 Marco de referencia para la gestión de la SI*

## LS2 Estructura y organización de la Seguridad de la Información

*LS2.1 Estructura del área de Seguridad de la Información [31] [37]*

*LS2.2 Autoridades de Seguridad de la Información [37] [31] [7]*

*LS2.3 Gestión de Activos de Información [37] [3] [31] [41]*

# LS1 ORGANIZACIÓN GENERAL DE LA SI

## *LS1.1 Contexto de la organización & Implementación del SMCSI*

**Objetivo** Establecer el entorno de la organización, detallando las cuestiones tanto internas como externas vinculadas a su naturaleza de negocio, que pudieran afectar su capacidad para alcanzar sus objetivos [3] [28].

| LS1.1.1 | Nivel E | F |
|---|---|---|
| Subproceso de generación del contexto externo | | |
| Establecer el contexto externo de la organización, el cual deberá considerar:<br><br>a) El contexto político, social y cultural, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo internacional, regional, nacional y local.<br>b) Valores y percepciones de las partes interesadas externas, y las relaciones de la organización con los mismos.<br>c) Tendencias y factores claves que influencian o pudieran influenciar los objetivos de la organización. | | |
| LS1.1.3 - LS1.1.4 | | |
| ISO 27.001 4.1 [3] – ISO 31.000 5.3.2 [28] | | |

| LS1.1.2 | Nivel E | F |
|---|---|---|
| Subproceso de generación del contexto interno | | |
| Establecer el contexto interno de la organización, el cual deberá considerar:<br><br>a) Gobierno, estructura organizacional, roles y responsabilidades.<br>b) Los objetivos y las políticas establecidas para alcanzarlos.<br>c) Capacidades de la organización en términos de recursos o conocimiento (Recursos Humanos, capital, tecnología, entre otros).<br>d) Cultura y valores de la organización.<br>e) Procesos de decisión y flujos de información, tanto formales como informales.<br>d) Normas y estándares adoptados por la organización.<br>e) Alcance y tipos de relaciones contractuales.<br>f) Sistemas de información d la organización.<br>g) Valores y percepciones de las partes interesadas internas, y las relaciones de la organización con los mismos. | | |
| LS1.1.3 - LS1.1.4 | | |
| ISO 27.001 4.1 [3] – ISO 31.000 5.3.3 [28] | | |

| LS1.1.3 | Nivel E | F |
|---|---|---|
| Subproceso de generación del contexto | | |
| Se debe determinar, en función del contexto generado en los requerimientos LS1.1.1 y LS1.1.2:<br><br>a) Las partes interesadas afectadas por el SMCSI.<br>b) Los requisitos de esas partes interesadas identificadas vinculados a la SI. | | |
| LS1.1.1 - LS1.1.2 | | |
| ISO 27.001 4.2 [3] – ISO 31.000 5.3 [28] | | |

| LS1.1.4 | Nivel E | F |
|---|---|---|
| Proceso del diseño del SMCSI<br><br>Subproceso de determinación del alcance | | |
| Se debe determinar el alcance del SMCSI, en función de lo generado en los Requerimientos LS1.1.1, LS1.1.2 y LS1.1.3 y, a su vez, tomando en cuenta las interfaces y dependencias entre los procesos ejecutados por la organización y aquellos ejecutados por otras organizaciones.<br><br>El alcance debe documentarse dentro de la PSI de la organización, con el objetivo de cumplir con el requisito 4.3 de la Norma ISO 27.001 [3].<br><br>Los estadios de madurez A y B solo serán compatibles con un alcance que cubra a la organización de extremo a extremo, incluyendo a todas las partes interesadas tanto internas como externas y, a su vez, a todos aquellos procesos y funciones que formen parte de la organización.<br><br>*Se recomienda priorizar a grandes rasgos los procesos de la organización en función de su criticidad y, acotar la primera implementación del SMCSI sobre aquellos considerados más críticos.* | | |
| LS1.1.1 - LS1.1.2 - LS1.1.3 | | |
| ISO 27.001 4.3 [3] – ISO 31.000 5.3.2 [28] – COBIT Principio 2 [22] | | |

| LS1.1.5 | Nivel E | F |
|---|---|---|
| Proceso del diseño del SMCSI | | |
| La organización debe diseñar un SMCSI acorde a su naturaleza y, a su vez, deberá establecerlo, implementarlo, mantenerlo y mejorarlo de forma continua en función de los requisitos del MRU y de sus propios objetivos estratégicos.<br><br>Se deberá considerar los requerimientos para el diseño del mismo detallados en el Dominio de SI GOB2.3.<br><br>*Cada organización moldeará su propio camino a lo largo del Modelo de Madurez de Seguridad de la Información establecido por el MRU, debido a que las metas de implementación del SMCSI, la operación y los objetivos de cada una no serán idénticos.* | | |

| GOB2.3 |
| --- |
| ISO 27.001 4.4 [3] |

| LS1.1.6 | Nivel E | F |
| --- | --- | --- |
| Proceso del diseño del SMCSI | | |
| El diseño e implementación del SMCSI de la organización deberá de ser abordado como un proyecto y llevado adelante en función de la metodología de gestión de proyectos utilizada por la organización.<br>Dicho proyecto deberá de tomar en cuenta los lineamientos detallados en los requerimientos LS1.1.7, LS1.1.8, LS1.1.9 y LS1.1.10.<br><br>*Los lineamientos se encuentran estructurados en función del nivel MRU seleccionado para la implementación correspondiente.* | | |
| LS1.1.7 - LS1.1.8 - LS1.1.9 - LS1.1.10 | | |
| ISO 27.001 4.4 [3] | | |

| LS1.1.7 | Nivel E | F |
| --- | --- | --- |
| Proceso del diseño del SMCSI | | |
| Se debe de diseñar y establecer un plan de proyecto de implementación del SMCSI que detalle lo siguiente:<br><br>a) Los objetivos de SI de la organización.<br>b) El promotor[50] del proyecto.<br>c) El responsable del desarrollo e implementación del proyecto (preferentemente el CISO de la organización).<br>d) El nivel actual de la organización con respecto al MMSI.<br>e) El nivel futuro del MMSI esperado a alcanzar.<br>d) Los niveles intermedios del MMSI a alcanzar como metas intermedias al estado futuro deseado.<br>e) Cronograma estratégico[51] de desarrollo del proyecto (se deben estimar e incluir metas e hitos de implementación). | | |

[50] Referencia al *"sponsor"* del proyecto de diseño e implementación del SMCSI.
[51] Descripción de dichas actividades con un nivel de abstracción significativo.

f) Recursos con los que contará el proyecto y su correspondiente presupuesto.
g) Alcance y visión del proyecto.
h) Justificación e importancia del proyecto.
i) identificación y tratamiento de riesgos del proyecto.

El Plan de proyecto deberá de ser firmado por el órgano rector de gobierno de gobierno de la organización, en concordancia con la metodología de gobierno establecida en GOB1.1.3.

*Cada organización moldeará su propio camino a lo largo del Modelo de Madurez de Seguridad de la Información establecido por el MRU, debido a que los objetivos, la operación y las metas de implementación del SMCSI de cada una no serán idénticos.*

*Para aquellas organizaciones de estrato III o inferiores, que no contarán con una estructura de gobierno, el plan de proyecto deberá de ser firmado por el CEO.*

| GOB1.1.3 |
|---|
| ISO 27.001 4.4 [3] – PMBOK [24] |

| LS1.1.8 | Nivel D | K |
|---|---|---|
| Proceso del diseño del SMCSI | | |

En función de los resultados de la implementación de los requerimientos LS1.1.1, LS1.1.2 y LS1.1.3 se determinarán los riesgos y oportunidades que deben tratarse, durante la planificación del SMCSI, para:

a) Asegurar que el SMCSI pueda lograr el o los resultados previstos.
b) Prevenir o reducir los efectos no deseados.
c) Lograr la mejora continua.

Luego se deberá planificar:

d) Las acciones para tratar las oportunidades y riesgos identificados anteriormente.
e) Como evaluar la eficacia de dichas acciones.
f) Como integrar e implementar dichas acciones dentro de los procesos del SMCSI dela organización.

| |
|---|
| Los resultados de la implementación del presente requerimiento serán incorporados en el plan de proyecto detallado en LS1.1.6.<br><br>*El presente requerimiento facilitará y favorecerá lograr una efectiva implementación del SMCSI dentro de la organización.* |
| LS1.1.6 - LS1.1.1 - LS1.1.2 - LS1.3 |
| ISO 27.001 6.1.1 [3] |

| LS1.1.9 | Nivel C | F |
|---|---|---|
| Proceso del diseño del SMCSI | | |
| El proyecto de implementación del SMCSI deberá de ser gestionado en función de un enfoque orientado a procesos en función de lo establecido en el SSI PM. | | |
| | | |
| ISO 27.001 4.4 [3] | | |

| LS1.1.10 | Nivel C | F |
|---|---|---|
| Proceso del diseño del SMCSI | | |
| Se deben de establecer métricas para monitorear y gestionar el desarrollo del proyecto de implementación del SMCSI. Dichas métricas deberán estar vinculadas con al menos los siguientes aspectos del proyecto:<br><br>a) Éxito del proyecto.<br>b) Porcentaje del proyecto implementado.<br>c) Desvíos de planificación.<br>d) Cumplimiento con la calidad de los entregables. | | |
| | | |
| ISO 27.001 4.4 [3] | | |

| LS1.1.11 | Nivel C | F |
|---|---|---|
| Subproceso de generación del contexto | | |
| Se deberá de documentar la necesidad de comunicaciones internas y externas pertinentes al SMCSI, detallando:<br><br>a) Que comunicar.<br>b) Cuando comunicar.<br>c) Con quien comunicarse.<br>d) Quien debe comunicar.<br>e) Los procesos mediante los cuales se va a realizar la comunicación.<br><br>El punto d) deberá ser concordante con lo establecido en LS2.2.<br>El punto e) deberá ser concordante con lo establecido en el subsistema PM.<br><br>Las actividades de comunicación deberán encontrarse especificadas en las responsabilidades de todos aquellos roles determinados en d). | | |
| | | |
| ISO 27.001 7.4 [3] | | |

[Página dejada en blanco intencionalmente]

## *LS1.2 Política de Seguridad de la Información*

**Objetivo** Proporcionar apoyo a la gestión de la SI de la organización y a su vez establecer una base de fundamento para todos los controles y medidas de SI que serán implementados [3].

| LS1.2.1 | Nivel D | F |
|---|---|---|
| Proceso de diseño de la PSI | | |
| Se deberá elaborar una PSI (Política de Seguridad de la Información), cuyo alcance deberá de corresponder al definido por la organización en LS1.1.4.<br><br>La PSI deberá ser de aplicación obligatoria para todo el personal de la organización.<br><br>*Se recomienda que la misma no supere las 10 carillas, ya que se perderá el entusiasmo de cualquier lector ejecutivo.* | | |
| LS1.1.4 | | |
| [31] – ISO 27.001 5.2 [3] – ISF Standard SM1.1.1 [41] | | |

| LS1.2.2 | Nivel D | F |
|---|---|---|
| Proceso de diseño de la PSI<br><br>Subproceso de gestión de requerimientos | | |
| La organización debe de identificar sus requerimientos de SI. Dichos requerimientos surgirán de: | | |

| |
|---|
| a) La gestión de riesgos de la organización.<br>b) Los requerimientos legales, contractuales, estatutarios y regulatorios que la organización, sus socios, contratistas, consultores y proveedores deben de cumplir.<br>c) El ambiente socio-cultural de la organización, sus socios, contratistas, consultores y proveedores.<br>d) El conjunto de principios, objetivos y requerimientos del negocio para el manejo, proceso, almacenamiento, comunicación y archivo de la información desarrollados por la organización para dar soporte a sus actividades.<br>e) La estrategia de negocio de la organización.<br>f) Entorno de amenazas de SI actual y proyectado. |
| |
| ISO 27.002 0.2 [7] |

| LS1.2.3 | Nivel C | F |
|---|---|---|
| Proceso de diseño de la PSI | | |
| La PSI debe:<br><br>a) Establecer claramente el SMCSI de la organización y su correspondiente alcance.<br>b) Ser debatida, aprobada y establecida por el CSI.<br>c) Ser aprobada y firmada por la máxima autoridad de la organización y por el órgano rector de gobierno de la misma.<br>d) Ser apropiada a la naturaleza y propósito de la organización.<br>e) Definir la SI y los objetivos y principios de SI que guiaran todas las actividades relacionadas a la SI de la organización.<br>f) Incluir los objetivos de SI o proporcionar un marco organizacional para el establecimiento y gestión de los mismos[52].<br>g) Detallar el compromiso de cumplimiento de los requisitos relativos a la SI de la organización establecidos en LS1.2.2.<br>h) Detallar el compromiso de cumplimiento por parte de las partes interesadas de los requisitos pertinentes establecidos en dicha política. | | |

[52] Ya que, en una primera implementación del SMCSI, serán delineados en función del requerimiento LS1.2.2 por el CSI luego de concluir el proceso de evaluación y tratamiento de riesgos.

i) Detallar la existencia y aplicación de sanciones ante el no cumplimiento de los requisitos pertinentes establecidos en la PSI.
j) Incluir el compromiso de mejora continua del SMCSI.
k) Establecer el CSI y su correspondiente responsabilidad.
l) Establecer la metodología de confección, aprobación y publicación de los manuales de procedimiento, guías, procesos, normas y políticas de SI de la organización.
m) Establecer el rol de las autoridades de SI detalladas en LS2.1 y LS2.2 y, a su vez, sus correspondientes responsabilidades.
n) Establecer al RT de la organización y su correspondiente responsabilidad.
o) Hacer referencia a procesos de manejo de desviaciones y excepciones.
p) Detallar sus objetivos y alcance.
q) Hacer referencia al resto de las políticas de SI (referirse a LS1.2.5).
r) Detallar los estándares de referencia tomados en cuenta para el desarrollo de la misma.
s) Hacer referencia a su vigencia y mantenimiento.
t) Detallar los principios de Si de la organización.

La PSI deberá ser de aplicación obligatoria para todas las partes interesadas internas de la organización (gerentes, propietarios y empleados) y, a su vez, para todos los usuarios de terceras partes de los AI de la organización y consultores o contratistas contratados por la misma.

*El cargo de RT debe de ser ocupado por la autoridad máxima de la organización referente a tecnología y sistemas de información.*

*En cuanto a k), m) y n) se recomienda que la descripción de las responsabilidades se mantenga al mínimo indispensable. La descripción detallada de las mismas se realizará en la política de autoridades (referirse a LS2.2.1) del MRU.*

*La PSI debe de ser revisada regularmente, tomando en cuenta las variables cambiantes del entorno.*

*Se deben de desarrollar políticas de uso aceptable que soporten a la PSI y definan la forma en que las partes interesadas son esperadas de utilizar la información, los sistemas y la conectividad de la organización.*

| LS1.1.4 –LS1.1.5 – LS1.2.2 – LS2.2.1 – LS1.2.5 |
|---|
| ISO 27.001 5.2, 4.4 y 4.3 [3] – PSI ONTI [37] – [22] - ISO 27.002 5.1.1 [7] - ISF Standard SM1.1.1, SM1.1.2, SM1.1.4 y SM1.2.1 [41] |

| LS1.2.4 | Nivel C | F |
|---|---|---|
| Proceso de diseño de la PSI<br><br>Subproceso de capacitación y concientización | | |
| Se deberán realizar acciones continuas de concientización y comunicación sobre la PSI, desde el comienzo de su armado y diseño. Dichas acciones serán mejoradas de forma continua, formarán parte del Programa de toma de conciencia, entrenamiento y difusión de la SI del SMCSI (PCED del SMCSI) y tomarán en consideración el requerimiento LS1.2.5).<br><br>*La PSI debe de ser comunicada a todas las partes interesadas de la organización.* | | |
| LS1.2.5 | | |
| ISO 27.001 5.2 [3] - ISF Standard SM1.1.4 [41] | | |

| LS1.2.5 | Nivel C | F |
|---|---|---|
| Proceso de diseño de Políticas MRU | | |
| En concordancia con el Control A.5.1.1 de la norma ISO 27.001 [3] y lo establecido en el apartado 5.1.1 de la norma ISO 27.002 [7], se establecerán otras políticas de SI, en adición a la PSI, que oportunamente serán detalladas en los SSI correspondientes. Dichas políticas serán de menor nivel que la PSI y se encontrarán orientadas a una cierta temática específica (como por ejemplo, la Política de Recursos Humanos, la Política de Gestión de accesos, la Política de escritorios y pantallas limpias, entre otras).<br><br>Estas políticas se basarán en la PSI de la organización y, al igual que esta, deberán:<br><br>a) Ser aprobadas por el CSI. Las revisiones a las distintas políticas a su vez, deberán de ser aprobadas por el CSI.<br>b) Ser publicadas y comunicadas a las partes interesadas internas y externas pertinentes dentro del Programa de toma de conciencia, entrenamiento y difusión de la SI del SMCSI (PCED del SMCSI).<br>c) Ser revisadas a intervalos planificados o si ocurren cambios significativos (como aquellos detallados en GR1.1.2) para asegurar que continúan siendo apropiadas, adecuadas y eficaces. Dentro de la revisión se deberán evaluar | | |

| |
|---|
| oportunidades de mejora de las distintas políticas y del enfoque de gestión de SI en función de aquellos cambios significativos detallados en GR1.1.2.<br>d) Tener un responsable asignado, quien tendrá responsabilidad por el desarrollo, revisión y evaluación de la política que se le ha asignado. El responsable por la PSI de la organización será el CISO.<br><br>*El presente requerimiento adhiere a los lineamientos detallados en la sección II capítulo 2.1 del Marco teórico COBIT, al proporcionar una estructura jerárquica a la que todas las políticas deben de ceñirse.* |
| GR1.1.2 |
| ISO 27.001 5.2 y control A.5.1.2 [3] – ISO 27.002 5.12 [7] – COBIT II.2.1 [22] |

| LS1.2.10 | Nivel C | K |
|---|---|---|
| Proceso de diseño de la PSI<br><br>Subproceso de capacitación y concientización | | |
| La PSI deberá publicarse y estar disponible como información documentada para todo el personal de la organización. De corresponder, estará a su vez disponible para las partes interesadas.<br><br>*Se deberán de realizar acciones de comunicación de la PSI a todas las partes interesadas de la organización.* | | |
| | | |
| ISO 27.001 5.2 [3] | | |

| LS1.2.7 | Nivel C | F |
|---|---|---|

Proceso de diseño de Políticas MRU

El marco de políticas de SI deberá respetar la siguiente estructura:

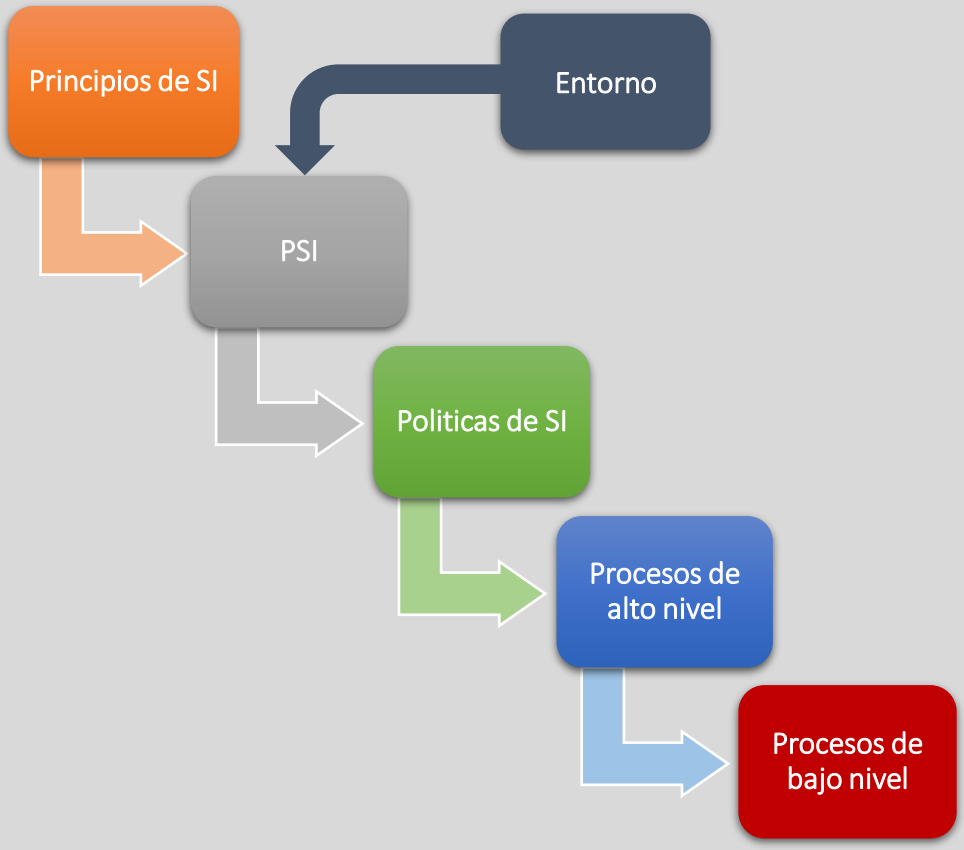



Ilustración LS1.2.6: Marco de Políticas COBIT [22]

Se deberá de establecer un marco de políticas de SI, que defina:

a) Las consecuencias de no cumplir con la política (en concordancia con LS1.2.3.i).
b) El ciclo de vida de las políticas de la organización.

El marco de políticas de SI de la organización deberá de ser desarrollado y mantenido por el CSI. El objetivo de dicho marco de referencia consiste en establecer un entorno base, en función de la metodología de cascada de metas, para el desarrollo de las políticas específicas de SI por parte de la organización.

El marco de políticas de SI, deberá de tomar como insumo, las siguientes variables del entorno:

a) Los principios de gobierno corporativos de la organización.
b) Los objetivos estratégicos de la organización.
c) La estrategia corporativa.
d) Apetito de riesgo de la organización (definido en GR1.1.3).
e) Estándares de la industria.
f) Políticas existentes dentro de la organización.
g) Regulaciones especificas a la organización.
h) Existencia de AES dentro de la organización.
i) Necesidades relativas a la protección de la propiedad intelectual e información competitiva.

*El motivo principal del establecimiento del marco de referencia recae en que les permite tanto a los destinatarios de las políticas de SI como a los profesionales de SI comprender como consultar las guías y documentos de SI disponibles. Por ejemplo, si surgiere un problema operativo se consultará la documentación de SI más detallada (los procesos de bajo nivel). En caso de que la documentación de bajo nivel no existiera o no evacue sus dudas, se procederá a consultar los procesos de alto nivel, luego las políticas de SI y así sucesivamente.*

*Las variables del entorno son una pieza fundamental a la hora de desarrollar las políticas de SI ya que, una organización con aversión al riesgo poseerá políticas totalmente diferentes a aquellas desarrolladas por una organización que asuma riesgos. A su vez, intervienen otras variables vinculadas a la naturaleza de la organización y el entorno en el que opera.*

COBIT II.2.1, 2.3 y 2.4 [22]

| LS1.2.8 | Nivel B | F |
|---|---|---|
| Proceso de diseño de Políticas MRU | | |
| El marco de políticas de SI, deberá de definir:<br><br>a) Los mecanismos para la gestión de las excepciones.<br>b) La forma en la que se comprobará y medirá el cumplimiento de la política. | | |
| COBIT II.2.1 [22] | | |

| LS1.2.9 | Nivel B | F |
|---|---|---|
| Proceso de diseño de Políticas MRU | | |
| Se deberá de definir y documentar un ciclo de vida de las políticas de SI. El cual deberá:<br><br>a) Requerir la evaluación y actualización de las políticas en forma regular.<br>b) Formalizar el proceso de desarrollo, implementación, mantenimiento y depreciación de las políticas de SI.<br><br>La organización deberá a su vez implementar un mecanismo desencadenante de actualizaciones por fuera del ciclo de vida de políticas de SI. | | |
| | | |
| COBIT II.2.1 [22] | | |

| LS1.2.10 | Nivel B | F |
|---|---|---|
| Proceso de diseño de Políticas MRU | | |
| La PSI debe:<br><br>a) Establecer el CEP y su correspondiente responsabilidad.<br>b) Hacer referencia a la medición de la eficacia y eficiencia de SI.<br>c) Requerir la generación de conciencia a los RRHH en cuanto a la SI y a su comportamiento de seguridad esperado. | | |
| | | |
| [3] – [22] – [31] - ISF Standard SM1.1.1 [41] | | |

| LS1.2.11 | Nivel B | F |
|---|---|---|
| Proceso de diseño de la PSI<br><br>Subproceso de capacitación y concientización | | |
| La PSI deberá ser de aplicación obligatoria para los clientes, proveedores, socios y cualquier tipo de entidad vinculada a la organización. Por lo que, será de aplicación y cumplimiento obligatorio para todas las partes interesadas. | | |

| |
|---|
| *La organización se encargará de delinear las formas de implementación y control del presente requerimiento. Se recomienda el establecimiento de PSI específicas para cada parte interesada detallada en el presente requerimiento.*<br><br>*En el caso de proveedores, socios y clientes se recomienda el desarrollo e implementación de una PSI especifica entre la organización y la parte interesada correspondiente.* |
| |
| |

| LS1.2.11 | Nivel B | F |
|---|---|---|
| Proceso de diseño de la PSI | | |
| Se deberá de establecer métodos que:<br><br>a) Permitan a los individuos confirmar su aceptación, entendimiento y cumplimiento de la PSI y las políticas de Si de la organización.<br>b) Evaluar el cumplimiento de las políticas de SI en forma regular.<br>c) Permitan a los individuos confirmar su aceptación y entendimiento de las acciones disciplinarias que podrían llegar a sufrir debido a violaciones en las políticas de SI. | | |
| | | |
| ISF Standard SM1.1.5 y 1.1.6 [41] | | |

[Página dejada en blanco intencionalmente]

## *LS1.3 Marco de Referencia para la gestión de la SI*

**Objetivo** Proporcionar un marco de referencia para la gestión y estructuración de la SI dentro de la organización, con el objetivo de facilitar la implementación, operación y control de la SI [7] [3].

| LS1.3.1 | Nivel D | F |
|---|---|---|
| Proceso de gestión de accesos de terceros | | |
| Se deberá de gestionar el acceso de terceros a la información de la organización. Se deberán de establecer PSI individuales con cada uno de los terceros que accederán a la información.<br><br>Dicha PSI deberá de tener en cuenta:<br><br>a) Asegurar la aplicación de medidas de SI adecuadas en los accesos de terceros.<br>b) La obligatoriedad del cumplimiento de la PSI, políticas y procesos de SI de la organización.<br>c) La gestión del cambio de dicha política.<br>d) Los procesos de inducción y comunicación de las terceras partes.<br>e) Gestión de riesgos especifica.<br>f) Acuerdos de confidencialidad y no divulgación.<br><br>*El diseño de dicha PSI se realizará en función de los recursos a acceder, los tipos de accesos, el valor de la información y los controles empleados por la tercera parte.* | | |
| | | |
| ISO 27.001 [3] – PSI ONTI [37] | | |

| LS1.3.1 | Nivel C | F |
|---|---|---|
| Proceso de definición de la estructura de SI | | |
| Las actividades y áreas de responsabilidades incompatibles deberán de ser segregadas, con el objetivo de reducir las oportunidades de modificaciones no autorizadas, no intencionales o el mal uso de los activos de la organización. Por lo tanto, la organización deberá de asegurarse que:<br><br>a) Ningún RRHH en forma individual pueda acceder, modificar o utilizar un activo de información la organización sin la debida autorización o sin ser detectado.<br>b) La acción de iniciación de un evento debe de encontrarse separada de la acción de su autorización.<br>c) Se contemple la posibilidad de colusión de responsabilidades durante el diseño de los controles de SI. | | |
| | | |
| ISO 27.001 A.6.1.2 [3] - ISO 27.002 6.1.2 [7] | | |

| LS1.3.2 | Nivel C | F |
|---|---|---|
| Proceso de definición de la estructura de SI<br><br>Subproceso de vínculos externos | | |
| Se deberán de establecer y mantener los contactos apropiados con las autoridades pertinentes, con el objetivo de facilitar y simplificar la implementación de los SSI de PD (relativo a incidentes de SI), de GC (relativo a la continuidad y contingencia de los activos de información de la organización) y de PM (relativo a la adaptación de la organización a nuevos cambios legales o regulatorios vinculados a la SI).<br><br>Se deberán de establecer contactos con:<br><br>a) El CERT nacional y local.<br>b) Organismos regulatorios pertinentes a la naturaleza de las actividades de la organización.<br>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), d) y e) podrán ser optativos para las implementaciones del SMCSI de aquellas organizaciones cuyo estrato sea menor a IV.*

*Si la organización es considerada una infraestructura crítica[53], en función de la Directiva 2008/114/CE del Consejo de la unión Europea [48], o contiene una de las áreas clasificadas como AES[54] 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 de los eventos y cuestiones de la 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]

[53] 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].
[54] Áreas de Extrema seguridad. Favor de referirse a la sección 3.1 del presente trabajo.

| LS1.3.3 | Nivel B | F |
|---|---|---|
| Proceso de definición de la estructura de SI<br><br>Subproceso de vínculos externos | | |
| Se deberán elaborar e implementar procesos que especifiquen:<br><br>a) Quien de la organización y en qué momento contactaran a las autoridades establecidas en LS1.3.2.<br>b) Como deberán de ser reportados de manera oportuna los incidentes de SI identificados por la organización. | | |
| | | |
| ISO 27.002 6.1.3 [7] - ISO 27.001 A.6.1.3 [3] | | |

| LS1.3.4 | Nivel B | F |
|---|---|---|
| Proceso de definición de la estructura de SI<br><br>Subproceso de vínculos externos | | |
| La organización deberá de ser miembro de aquellos grupos o foros de interés especial detallados en LS1.3.2.f con el objetivo de:<br><br>a) Perfeccionar el conocimiento de mejores prácticas en la materia y mantenerse al día con la información de seguridad relevante.<br>b) Asegurar que la comprensión del entorno de la SI es actual y completa.<br>c) Recibir alertas tempranas, avisos, recomendaciones y parches relacionados con nuevos ataques y vulnerabilidades.<br>d) Obtener acceso a asesoramiento especializado en la temática.<br>e) Obtener y compartir información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades.<br>f) Proporcionar puntos de enlace adecuados cuando se enfrenten incidentes de SI.<br>g) Cultivar vínculos.<br>h) Adquirir nuevos conocimientos. | | |
| | | |
| ISO 27.002 6.1.4 [7] – ISO 27.001 A.6.1.4 [3] | | |

| LS1.3.5 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| La SI deberá de integrarse con la metodología de gestión de proyectos de la organización para asegurar que los riesgos de SI son identificados y abordados, como parte de cualquier proyecto emprendido por la organización. Para lo cual, se deberá:<br><br>a) Incluir dentro de los objetivos del proyecto, objetivos de SI.<br>b) Realizar una evaluación de riesgos de SI en una etapa temprana del proyecto con el objetivo de identificar controles necesarios.<br>c) Asegurar que la SI forma parte de todas las fases de la metodología de gestión de proyectos aplicada por la organización.<br>d) Asegurar que las implicaciones de SI son abordadas y revisadas regularmente en todos los proyectos de la organización.<br>e) Definir roles dentro de los proyectos que contengan ciertas responsabilidades específicas de SI para asegurar la correcta implementación del presente requerimiento. | | |
| | | |
| ISO 27.002 6.1.5 [7] – ISO 27.001 A.6.1.5 [3] | | |

| LS1.3.6 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| Los proyectos de SI deberán:<br><br>a) Ser ejecutados de una forma estructurada, sistemática y consistente, en línea con la metodología de gestión de proyectos de la organización.<br>b) Tener un alcance claramente definido, documentado y aprobado.<br>c) Conformar parte de un programa anual de seguridad.<br>d) Establecer claramente como el mismo colaborará en el logro de los objetivos de negocio, en la obtención de beneficios para la organización y en el alineamiento con la estrategia de SI.<br>e) Incluir requerimientos de recursos y presupuesto.<br>f) Proveer una indicación sobre el retorno de inversión esperado. | | |
| | | |
| ISF Standard SM 2.2.2 y SM2.2.5 [41] | | |

| LS1.3.7 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| Se deberán de ejecutar una amplia gama de proyectos de SI parar colaborar en:<br><br>a) Alineamiento de la SI con los procesos de negocio.<br>b) Cumplimientos de los requerimientos de las partes interesadas.<br>c) Permitir iniciativas de negocio.<br>d) Mejorar la eficiencia y eficacia de la SI a través de toda la organización. | | |
| | | |
| ISF Standard SM 2.2.1 [41] | | |

| LS1.3.8 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| El CSI será responsable de supervisar la ejecución de los proyectos de SI. El CEP será responsable de gestionarlos. El CSI será responsable de la gestión de los programas de SI. | | |
| | | |
| ISF Standard SM 2.2.3 [41] | | |

| LS1.3.9 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| En función de LS1.3.8, el CEP será responsable por:<br><br>a) Aprobar cada plan de proyecto.<br>b) Asignar a un sponsor de la dirección ejecutiva para cada proyecto.<br>c) Identificar y colaborar en el reclutamiento de RRHH con la experiencia y habilidades necesarias.<br>d) Asignar un líder de proyecto (PM), quien será responsable por el mismo.<br>e) Asegurar el establecimiento de los objetivos del proyecto.<br>f) Verificando que las actividades del proyecto adhieren a las políticas y estándares de la organización. | | |

| |
|---|
| g) Asegurando que las actividades del proyecto cumplen con las regulaciones, normas y estándares externos.<br>h) Monitoreando el estado de cada proyecto.<br>i) Comunicando regularmente el estado de los proyectos a las partes interesadas. |
| |
| ISF Standard SM 2.2.4 [41] |

| LS1.3.10 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| Los proyectos de SI deberán de tomar en cuenta:<br><br>a) La infraestructura de TI.<br>b) Arquitectura de SI.<br>c) Percepción del valor de la SI.<br>d) Sector de la industria, tipo de negocio, cultura y apetito de riesgo.<br>e) Políticas, estándares y guías de SI.<br>f) Uso y necesidad de proveedores. | | |
| | | |
| ISF Standard SM 2.2.5 [41] | | |

| LS1.3.11 | Nivel B | F |
|---|---|---|
| Proceso de gestión de proyectos de SI | | |
| Los proyectos de SI deberán ser monitoreados regularmente para asegurar que:<br><br>a) Identifican riesgos y cuestiones o incidentes.<br>b) Entregar los beneficios establecidos.<br>c) Logran los objetivos de SI y del negocio.<br>d) Adhieren a las definiciones aprobadas de alcance.<br>e) Poseen una correcta gestión de cambios y desvíos. | | |
| | | |
| ISF Standard SM 2.2.6 [41] | | |

| LS1.3.12 | Nivel B | F |
|---|---|---|
| Subproceso de gestión de requerimientos | | |
| Los requerimientos establecidos en LS1.2.2 que afectan a la SI deben de ser reconocidos por:<br><br>a) La dirección ejecutiva.<br>b) Los gerentes de negocio.<br>c) El CISO.<br>d) Todos aquellos miembros de la organización que forman parte del CSI, CEP y EGR. | | |
| LS1.2.2 | | |
| ISF Standard SM 2.3.1 [41] | | |

| LS1.3.13 | Nivel B | F |
|---|---|---|
| Subproceso de gestión de requerimientos | | |
| Se debe establecer un proceso para asegurar el cumplimiento de los requerimientos establecidos en LS1.2.2 (*proceso de compliance*). El mismo deberá de alcanzar:<br><br>a) Legislación específica en SI (código penal por ejemplo).<br>b) Legislación general que posee implicancias en seguridad (ley de datos personales por ejemplo).<br>c) Regulaciones de la industria y/o mercado (PCI DSS por ejemplo). | | |
| LS1.2.2 | | |
| ISF Standard SM 2.3.2 [41] | | |

| LS1.3.14 | Nivel B | F |
|---|---|---|
| Subproceso de gestión de requerimientos | | |
| El proceso de compliance debe de:<br><br>a) Encontrarse documentado.<br>b) Ser firmado por la dirección ejecutiva. | | |

| |
|---|
| c) Mantenerse al día. |
| |
| ISF Standard SM 2.3.4 [41] |

| LS1.3.15 | Nivel B | F |
|---|---|---|
| Subproceso de gestión de requerimientos | | |
| El proceso establecido en LS1.3.13 debe permitir a los tomadores de decisiones:<br><br>a) Identificar leyes y regulaciones vinculadas a la SI que afectarán a la organización.<br>b) Interpretar las implicancias e impacto que las leyes y regulaciones descubiertas en a) tendrán en la SI de la organización.<br>c) Identificar y solucionar posibles incumplimientos legales y regulatorios. | | |
| LS1.3.13 | | |
| ISF Standard SM 2.3.3 [41] | | |

| LS1.3.16 | Nivel B | F |
|---|---|---|
| Subproceso de gestión de requerimientos | | |
| Se deberá de realizar una revisión del cumplimiento de los requerimientos detallados en LS1.2.2. Dicha revisión deberá:<br><br>a) Desarrollarse regularmente y siempre que entren en vigencia nuevos requerimientos.<br>b) Involucrar a representantes de las áreas claves de la organización (dirección ejecutiva, dueños de productos, área de legales, de TI o de RRHH, entre otras).<br>c) Resultar en la actualización de políticas y procesos de SI con el objetivo de amoldarlos a cualquier cambio necesario. | | |
| LS1.2.2 | | |
| ISF Standard SM 2.3.5 [41] | | |

[Página dejada en blanco intencionalmente]

# LS2 ESTRUCTURA Y ORGANIZACIÓN DE LA SI

## *LS2.1 Estructura del área de Seguridad de la Información*

**Objetivo** Establecer los lineamientos básicos y fundamentales a ser tomados en cuenta a la hora de diseñar, desarrollar, implementar y mejorar una estructura de SI.

| LS2.1.1 | Nivel D | K |
|---|---|---|
| Proceso de definición de la estructura de SI | | |
| Todos los roles, responsabilidades y principios operativos de SI deberán de encontrarse bien definidos y documentados.<br><br>A su vez, deberán de ser comunicados de forma efectiva a todas las partes interesadas y deberán de encontrarse siempre disponibles para las mismas. | | |
| | | |
| COBIT II 4.1 [22] - [4] – ISF Standard SM2.1.1 [41] | | |

| LS2.1.2 | Nivel C | K |
|---|---|---|
| Proceso de definición de la estructura de SI | | |
| La organización deberá delinear e implementar una estructura de SI acorde a los lineamientos establecidos en el presente Dominio de SI y en el SSI ON. A su vez, deberá de definir y documentar el ciclo de vida de la misma.<br><br>*Debe de tomarse en cuenta que la posición dentro de la estructura de la organización del área de SI conforma un factor clave a la hora de determinar la capacidad de la organización para proteger su información. Esta posición establece la diferencia entre un área de SI alineada de forma proactiva con el negocio y otra que consiste en acciones de emergencia y de último minuto para mitigar el riesgo que se ha materializado.*<br><br>*La estructura debe de ser revisada regularmente.* | | |
| | | |
| COBIT II 4.1 [22] - COBIT II 4.3 [22] – ISF Standard SM2.1.7.e [41] | | |

| LS2.1.3 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI | | |
| Se debe de establecer una política de autoridades de SI (en función del requerimiento LS1.2.7). Dicha política debe establecer las funciones y la responsabilidad de:<br><br>a) El CISO.<br>b) SOO.<br>c) Los RAIs.<br>d) Los RGs.<br>e) El RASI.<br>f) Custodio de AI.<br>g) El RT.<br>h) CIPO.<br>i) RMO.<br>j) Los RPs. | | |

La política deberá de detallar que las autoridades de SI podrán delegar parcialmente o totalmente sus facultades, no obstante continuaran siendo responsables por el cumplimiento en forma eficiente y eficaz de dichas facultades.

El establecimiento de las responsabilidades de las autoridades de SI deberá realizarse de forma concordante con los requerimientos del MRU, el SMCSI de la organización y sus políticas de SI.

La organización deberá de establecer un proceso de asignación y comunicación de las responsabilidades establecidas en la política de autoridades de SI. Dicho proceso deberá encontrarse debidamente documentado.

*Dentro de dicha política se debe de establecer la diferencia en cuanto a los roles específicos de SI (CISO, SOO, RAIs, RT, entre otros) y aquellos vinculados con la SI (RGs, CEO, CIO, CTO, entre otros).*

[3] - 27.002 6.1.1 [7] - COBIT II 4.1 [22]

| LS2.1.4 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br>Subproceso de RPs | | |
| El CSI deberá de establecer RPs por cada uno de los procesos de SI de la organización. Los RP serán responsables por:<br><br>a) La eficiente y eficaz ejecución del proceso a su cargo.<br>b) Por el mantenimiento, revisión y mejora continua del proceso a su cargo.<br>c) Por el mantenimiento adecuado, correcto y exacto de la documentación de los procesos a su cargo.<br>d) La disponibilidad de la documentación mencionada en c).<br>e) La capacitación de todos los actores intervinientes en el proceso a su cargo. | | |

| LS2.1.5 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br><br>Subproceso de RASI | | |
| Se deberá de establecer un RASI, el cual contará con la responsabilidad de la planificación y desarrollo de auditorías periódicas de SI del SMCSI de la organización. Será a su vez responsable de presentar los resultados de dichas auditorias ante el CSI.<br><br>El RASI auditará la conformidad del SMCSI de la organización con los requerimientos del MRU, con el objetivo del relevamiento, búsqueda de no conformidades e identificación de oportunidades de mejora.<br><br>El RASI se encontrará a cargo del área de auditoria de SI de la organización y rendirá cuentas ante el CEO de la organización.<br><br>El RASI deberá registrar y documentar todas sus actividades.<br><br>*El RASI podrá de rendir cuentas ante el responsable global de auditoria de la organización, siempre y cuando este dependa directamente del CEO de la organización.*<br><br>*Se recomienda que el RASI sea considerado un miembro permanente del CSI, CEP y EGR con el objetivo de colaborar en cuanto a evitar la ocurrencia de no conformidades. El RASI podrá emitir recomendaciones pero no podrá gestionar ni participar en las decisiones de dichas estructuras de Gobierno de SI (posee voz pero no voto).*<br><br>*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.* | | |
| | | |
| [31] – PSI ONTI [37] – [4] – [3] | | |

| LS2.1.6 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br><br>Subproceso de RAIs y Custodios de AI | | |
| En función de LS2.3.10, la organización deberá de establecer RAIs para cada AI identificado dentro del proceso de gestión de activos de información (establecido en LS2.3.11).<br><br>Los RAI serán responsables por:<br><br>a) Implementar los requisitos del SMCSI durante todo el ciclo de vida de la información (establecido en LS2.3.2).<br>b) Gestionar adecuadamente los riesgos a lo largo de todo el ciclo de vida de la información, incorporando cambios y modificaciones ante la mutación de dichos riesgos a lo largo del tiempo.<br>c) El manejo adecuado y responsable del AI durante todo el ciclo de vida del mismo.<br>d) Asegurar que los AI bajo su responsabilidad se encuentran inventariados.<br>e) Asegurar que los AI bajo su responsabilidad sean clasificados (en función de los niveles de confidencialidad, integridad, disponibilidad y criticidad establecidos por el CSI en LS2.3.13) y protegidos adecuadamente.<br>f) Asegurar el manejo adecuado del AI, cuando este sea destruido o eliminado.<br>g) Definir y revisar periódicamente los derechos de acceso y clasificaciones de los AI bajo su responsabilidad, en función de la política de gestión de accesos de la organización.<br>h) Documentar la clasificación de los AI a su cargo y mantener dicha documentación actualizada en todo momento.<br>i) Informar sobre cualquier cambio que afecte el inventario de activos.<br>j) Definir los requerimientos de SI de los AI.<br>k) Velar por la implementación y mantenimiento de los controles de SI requeridos.<br><br>Los RAI deben de contar con la responsabilidad de gestión aprobada del ciclo de vida del activo por el cual son responsables.<br><br>La asignación de los derechos de acceso debe de realizarse en concordancia con las funciones y competencia de cada usuario final (en función de lo establecido en LS2.3.17). | | |

| |
|---|
| Se deberá a su vez definir y establecer a los custodios de los AI de la organización y sus correspondientes responsabilidades.<br><br>*Los RAI podrán formar parte del CSI, CEP y EGR con el objetivo de que comuniquen tanto iniciativas de negocio que puedan impactar en SI como el impacto que las prácticas de SI pueden causar a los usuarios de la organización. Esto se debe que los RAI son quienes comprenden los riesgos del negocio.*<br><br>*El RAI de la PSI de la organización deberá de ser el CISO, ya que este es responsable por su desarrollo, evaluación y mejora continua.* |
| LS2.3.10 – LS2.3.2 – LS2.3.11 – LS2.3.17 |
| ISO 27.002 0.5 y 8.1.2 [7] – PSI ONTI [37] – COBIT apéndice C [22]<br>ISO 27.001 A.8.1.2, A.8.1.3 y A.9.2.5 [3] |

| LS2.1.7 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br><br>Subproceso de RAIs y Custodios de AI | | |
| La revisión de los derechos de acceso establecida en LS2.2.6.g deberá de considerar lo siguiente:<br><br>a) Los privilegios de accesos deben ser revisados a intervalos regulares y luego de cualquier tipo de cambio (ascenso, cambio de rol, despido, etc.).<br>b) Las asignaciones de accesos privilegiados deben de revisarse regularmente con el objetivo de asegurarse que no se han obtenido privilegios no autorizados.<br>c) Las asignaciones de accesos privilegiados deben ser revisadas a intervalos significativamente más frecuentes que otras asignaciones de accesos.<br>d) Los cambios relativos a las cuentas de acceso privilegiado deben registrarse con el objetivo de ser auditados periódicamente. | | |
| LS2.2.6.g | | |
| ISO 27.001 A.9.2.5 [3] - ISO 27.002 9.2.5 [7] | | |

| LS2.1.8 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br>Subproceso de RMO | | |
| La organización deberá de establecer un área de RMO[55] (“*Oficina de gestión de riesgos*”).<br><br>El titular de la RMO se encargará de realizar una eficiente y efectiva gestión de los riesgos de SI de la organización y de la supervisión del proceso de gestión de AI. A su vez, rendirá cuentas ante el CISO de la organización.<br><br>*El RMO podrá de rendir cuentas ante el responsable global de riesgos de la organización, siempre y cuando este dependa directamente del CEO de la organización.*<br><br>*Se recomienda que el RMO sea considerado un miembro permanente del CSI, CEP y EGR.*<br><br>*Se recomienda que el CISO delegue en forma parcial el proceso de gestión de riesgos al RMO, siempre conservando la supervisión del mismo.* | | |

| LS2.1.9 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br>Subproceso de CIPO | | |
| La organización deberá de establecer un área de CIPO[56] (“*Oficina de Procesos y Mejora Continua*”). El titular del CIPO se enfocará en:<br><br>a) La investigación y desarrollo de SI.<br>b) La gestión de la mejora continua del SMCSI.<br>c) Desarrollo de mejoras y su planificación en conjunto con el CISO y SOO. El CIPO diseña cambios y releva las mejores prácticas y DF en la materia.<br>d) Apoyo al SOO en las implementaciones de las mejoras mencionadas en c). | | |

[55] “*Risk Management Office*” por sus siglas en inglés.
[56] “*Risk Management Office*” por sus siglas en inglés.

e) La incorporación de nuevos requerimientos de SI.
f) Desarrollo, implementación y mantenimiento del PCED.
g) Coordinación y realización de todas las actividades, seminarios, reuniones, capacitaciones, etc. periódicas para todas las partes interesadas que comprende el PCED.
h) La adecuación de los procesos de inducción del nuevo personal de la organización a los requerimientos de SI.
i) Relevar, diseñar, desarrollar, mantener y mejorar de forma continua los procesos de SI de la organización.
j) Colaborar en las revisiones de las políticas y procesos de SI y, proponer cambios en las mismas.

[3] – PSI ONTI [37] – [41] – [31] – ISF Standard SM2.1.3.b

| LS2.1.10 | Nivel C | F |
|---|---|---|

Proceso de establecimiento de autoridades de SI

Subproceso de SOO

La organización deberá de establecer un área de SOO[57] ("*Oficina de operaciones de Seguridad*"). El titular del SOO no se enfocará en la gestión de firewalls, IDS/IPS, gestión de credenciales o cualquier otro tipo de actividad operativa de seguridad (dichas actividades serán llevadas adelante por el RT de la organización).

El titular de la SOO se encargará de:

a) Supervisión de la eficiencia y eficacia de todos los controles de SI de la organización.
b) La gestión de incidentes de SI (supervisará la investigación y resolución de incidentes).
c) La gestión de la continuidad del negocio.
d) La implementación de los cambios delineados por el CIPO, en conjunto con esté.
e) Ser el punto de contacto con el SOC de la organización.

[57] "*Risk Management Office*" por sus siglas en inglés.

f) Llevar adelante la MSI (matriz de SI) que delinea todos los controles implementados por la organización (detallando tipo de control, responsable, matriz RACI asociada y métricas vinculadas).
g) Diseñar, establecer, gestionar, mantenerse y mejorar el equipo de gestión de incidentes de SI.
h) La gestión de los controles y los procesos de SI.
i) Traducir ("*bajar a tierra*") las políticas de SI de la organización en procesos (tanto de alto como de bajo nivel).

A su vez, rendirá cuentas ante el CISO de la organización.

*Se recomienda que el SOO forme parte del CSI con el objetivo de debatir las soluciones de diseño de SI por adelantado con los RAI y los arquitectos de SI.*

ISF Standard SM2.1.2.g [41]

| LS2.1.11 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br>Subproceso de RT | | |
| El CSI se encargará de nombrar a un RT (Responsable de Tecnología y Sistemas). Se recomienda que el mismo consista en la máxima autoridad en cuanto a tecnología y sistemas de la organización (CIO, CTO o similares).<br><br>*El nombramiento de RAI tiene por único objetivo identificar a un responsable de TI en cuanto a la implementación de ciertos requerimientos del SMCSI.* | | |

| LS2.1.12 | Nivel C | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br>Subproceso de RGS | | |
| El CSI deberá de establecer quienes dentro de la estructura de la organización serán considerados RGs (responsables gerenciales). | | |

*El nombramiento de RGs tiene por único objetivo identificar a los responsables titulares de las divisiones, secciones o áreas de la organización en cuanto a la implementación de ciertos requerimientos del SMCSI.*

| LS2.1.13 | Nivel C | F |
|---|---|---|

Proceso de definición de la estructura de SI

La organización deberá de implementar una estructura de 4 líneas de defensa:

a) RMO.
b) SOO.
c) CIPO.
d) Auditoria de SI.

*Se incluye a continuación un marco de estructura de SI acorde a todos los requerimientos detallados anteriormente.*

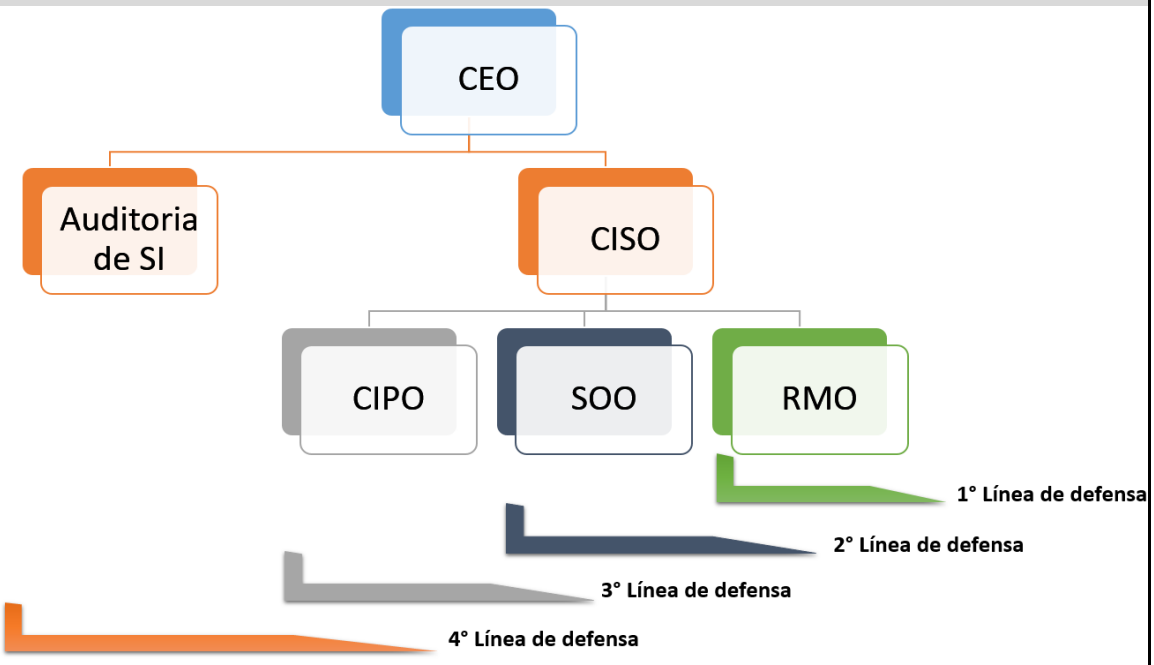



Ilustración LS2.1.13.A: estructura jerárquica de las líneas de defensa MRU.

| LS2.1.14 | Nivel B | F |
|---|---|---|
| Proceso de establecimiento de autoridades de SI<br><br>Subproceso de CIPO | | |
| El CIPO de la organización será responsable por el diseño, implementación y mantenimiento del tablero de gestión de SI. El mismo será diseñado en función de los KPIs[58] establecidos por el CISO (los cuales deben de ser derivados en formato cascada de los objetivo de SI definidos por el CSI).<br><br>El SOO será responsable por la gestión y alimentación de dicho tablero. | | |
| | | |
| | | |

| LS2.1.15 | Nivel B | F |
|---|---|---|
| Proceso de definición de la estructura de SI | | |
| Se deberá de definir un mandato (las razones y el propósito de su existencia) de la estructura de SI definida por la organización.<br><br>El área de SI deberá de contar con una influencia suficiente sobre toda la organización y, sobre todo, son un fuerte apoyo de la dirección ejecutiva, gerentes de negocio y de TI. | | |
| | | |
| COBIT II 4.1 [22] – ISF Standard SM2.1.7 [41] | | |

| LS2.1.16 | Nivel B | F |
|---|---|---|
| Proceso de definición de la estructura de SI | | |
| La máxima autoridad a cargo del área de legales o asuntos jurídicos de la organización tendrá la responsabilidad de:<br><br>a) Brindar asesoría en materia legal a cualquier autoridad de SI o estructura de gobierno de SI. | | |

[58] Traducción del inglés KPIs: "*Key Performance Indicators*".

| |
|---|
| b) Verificar el cumplimiento de los requerimientos del SMCSI en los diferentes contratos o acuerdos suscriptos por la organización. |
| |
| PSI ONTI [37] – [4] – [31] |

| LS2.1.17 | Nivel B | F |
|---|---|---|
| La organización deberá de implementar un equipo Tango (equipo de seguridad ofensiva), que será responsable de realizar pruebas, simulaciones y ejercicios de seguridad ofensiva (tanto técnicos como de ingeniería social). A su vez, serán responsables de realizar capacitaciones ofensivas.<br><br>Los resultados de estas pruebas serán utilizados como base para la mejora continua del SMCSI de la organización. | | |
| | | |

| LS2.1.18 | Nivel B | F |
|---|---|---|
| El área de SI de la organización deberá de convertirse en un centro de mejora continua para la SI en a través de:<br><br>a) Proveer asistencia experta en aspectos vinculados a SI y Ciberseguridad.<br>b) La incorporación de los requerimientos de SI dentro de acuerdos documentados (por ejemplo: contratos y SLAs) y el desarrollo de términos y condiciones.<br>c) Proveer el soporte para la protección de la información asociada con sistemas especializados[59].<br>d) La Evaluación de las implicaciones de iniciativas especializadas de negocio (por ejemplo: outsourcing, intercambio de información, iniciativas de comercio electrónico, entre otras).<br>e) La participación en el intercambio de información de inteligencia sobre Ciberamenazas y colaboración con sus "*cyber-partners*"[60]. | | |
| | | |
| ISF Standard SM2.1.3 [41] | | |

[59] Por ejemplo: sistemas vinculados a IoT y sistemas de control industrial (SCADA, DCS y PLC).
[60] Por ejemplo: ISPs, analistas de seguridad, organismos reguladores de la industria, entre otros.

| LS2.1.19 | Nivel B | F |
|---|---|---|

Proceso de definición de la estructura de SI

La organización deberá de implementar una estructura de 5 líneas de defensa:

a) MRO.
b) SOO.
c) CIPO.
d) Auditoria de SI.
e) Equipo Tango.

*Se incluye a continuación un marco de estructura de SI acorde a todos los requerimientos detallados anteriormente.*

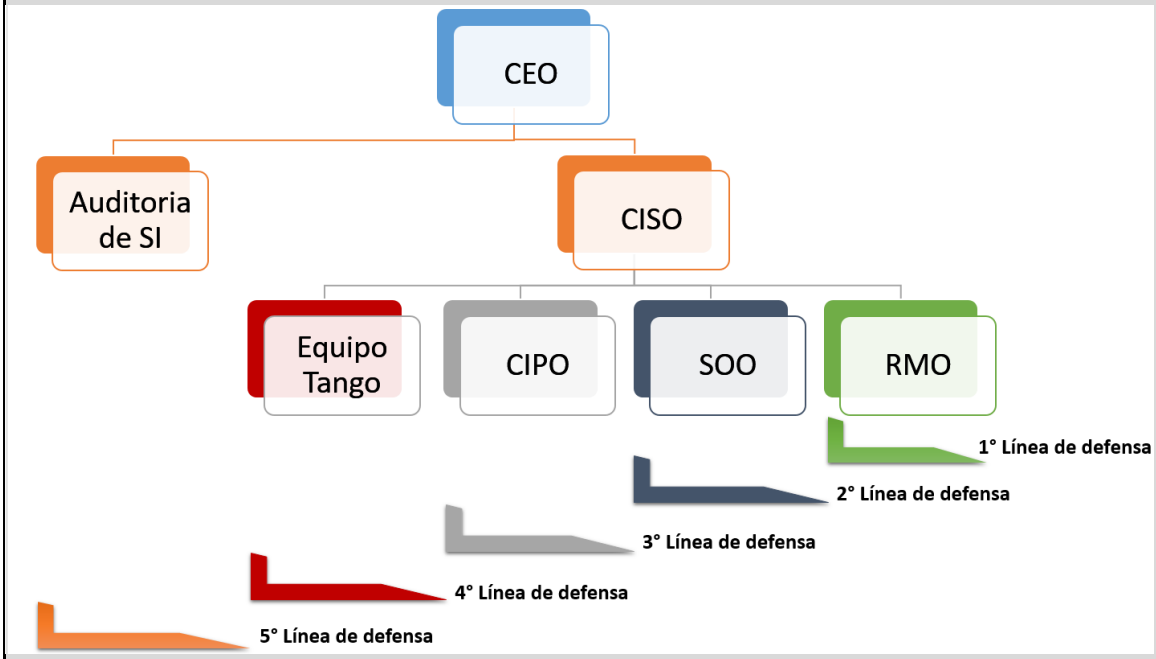



Ilustración LS2.1.18.A: estructura jerárquica de las líneas de defensa MRU.

| LS2.1.20 | Nivel A | F |
|---|---|---|
| Se deberán realizar auditorías independientes periódicas sobre la conformidad del SMCSI de la organización con los requerimientos del MRU. | | |
| | | |

| LS2.1.21 | Nivel A | F |
|---|---|---|
| El área de SI deberá de contar con los recursos adecuados en términos de:<br><br>a) El número y tipo de RRHH dedicados a SI.<br>b) El rango y nivel de habilidades de los RRHH detallados en a).<br>c) Herramientas y técnicas. | | |
| | | |
| ISF Standard SM2.1.6 [41] | | |

| LS2.1.22 | Nivel A | F |
|---|---|---|

Proceso de definición de la estructura de SI

La organización deberá de implementar una estructura de 6 líneas de defensa:

a) MRO.
b) SOO.
c) CIPO.
d) Auditoria de SI.
e) Equipo Tango.
f) Auditoria externa.

*Se incluye a continuación un marco de estructura de SI acorde a todos los requerimientos detallados anteriormente.*

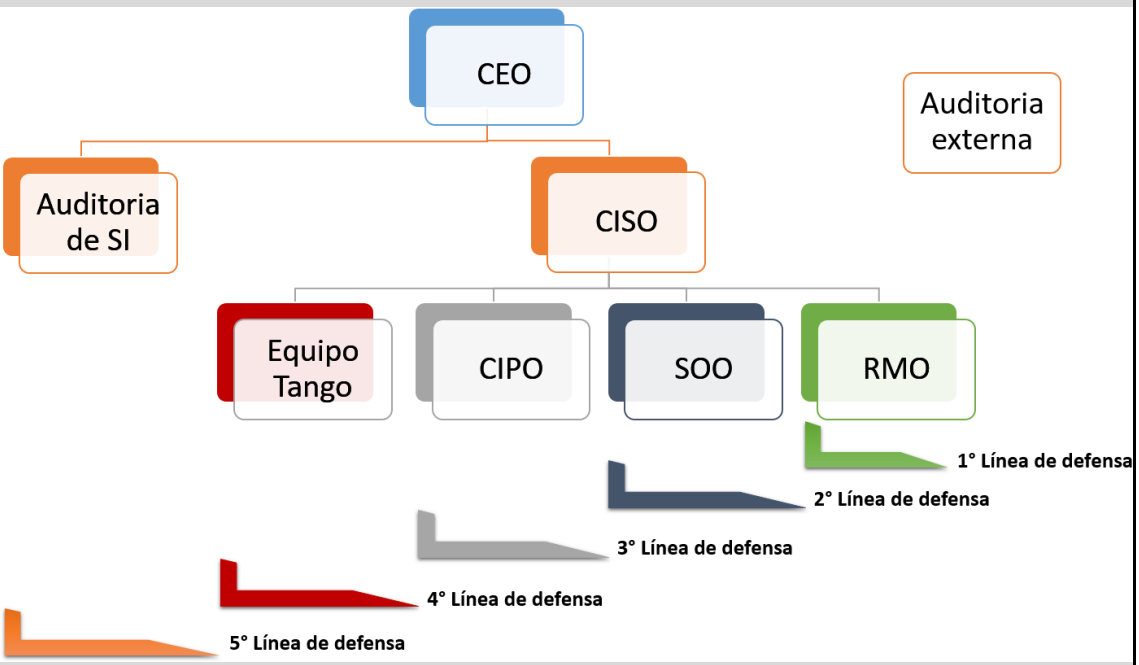



Ilustración LS2.1.21.A: estructura jerárquica de las líneas de defensa MRU.

[Página dejada en blanco intencionalmente]

## *LS2.2 Estructura de Gobierno de SI*

**Objetivo** Establecer los lineamientos generales en cuanto a la estructura de Gobierno de SI de la organización. Dichos lineamientos conforman un complemento de bajo nivel a lo establecido en el Dominio de SI GOB1.4.

| LS2.2.1 | Nivel D | F |
|---|---|---|
| Macroproceso de estructura de Gobierno de SI<br>Subproceso de establecimiento del EGR | | |
| Se deberá establecer un EGR (Equipo de gestión de riesgos) dentro de la organización. El mismo deberá estar integrado por:<br><br>a) RMO, quien coordinará el accionar del EGR.<br>b) Gerentes funcionales de las áreas sujetas a análisis (RGs) y RAIs vinculados.<br>c) Representantes seleccionados por los responsables máximos de las áreas de RRHH, legales, riesgos, TI, PMO y auditoria.<br>d) El RT de la organización.<br>e) SOO.<br><br>*En cuanto a los miembros detallados en b), los mimos mutarán constantemente debido a la necesidad de incorporar a la gestión de riesgos a aquellos RGs y RAIs considerados responsables por los riesgos y AI bajo análisis.*<br><br>*Los miembros detallados en c) podrán ser considerados miembros permanentes o invitados a participar cuando el coordinador del EGR lo requiera. Cada organización seleccionará la metodología que crea acorde a su naturaleza.* | | |

| |
|---|
| *El EGR es responsable de la toma de decisiones para evaluar, controlar, optimizar, financiar y monitorizar los riesgos de SI con el propósito de incrementar el valor generado por la organización para las partes interesadas.* |
| |
| COBIT II 4.2 [22] |

| LS2.2.2 | Nivel C | F |
|---|---|---|
| Macroproceso de dirección estrategia de la SI<br>Subproceso de establecimiento del CSI | | |
| En función del requerimiento GOB1.4.5.f, el presidente del CSI:<br><br>a) Es responsable de coordinar las actividades y reuniones del CSI.<br>b) Es responsable del cumplimiento de los requerimientos GOB1.4.5 y GOB.1.4.6.<br><br>*Cada organización podrá optar por brindarle tanto al presidente del CSI como al CISO el poder de veto de las decisiones del CSI.* | | |
| GOB1.4.5.f | | |
| | | |

| LS2.2.3 | Nivel B | F |
|---|---|---|
| Macroproceso de dirección estrategia de la SI<br>Subproceso de establecimiento del CEP | | |
| Se deberá establecer un CEP (Comité Ejecutivo Permanente) de SI dentro de la organización. El Comité deberá estar integrado por:<br><br>a) SOO que ocupará el rol de presidente del CEP.<br>b) Un representante del CEO de la organización.<br>c) Representantes seleccionados por los responsables máximos de las áreas de RRHH, legales, riesgos, TI y auditoria.<br>d) RMO.<br>e) RASI.<br>f) CIPO. | | |

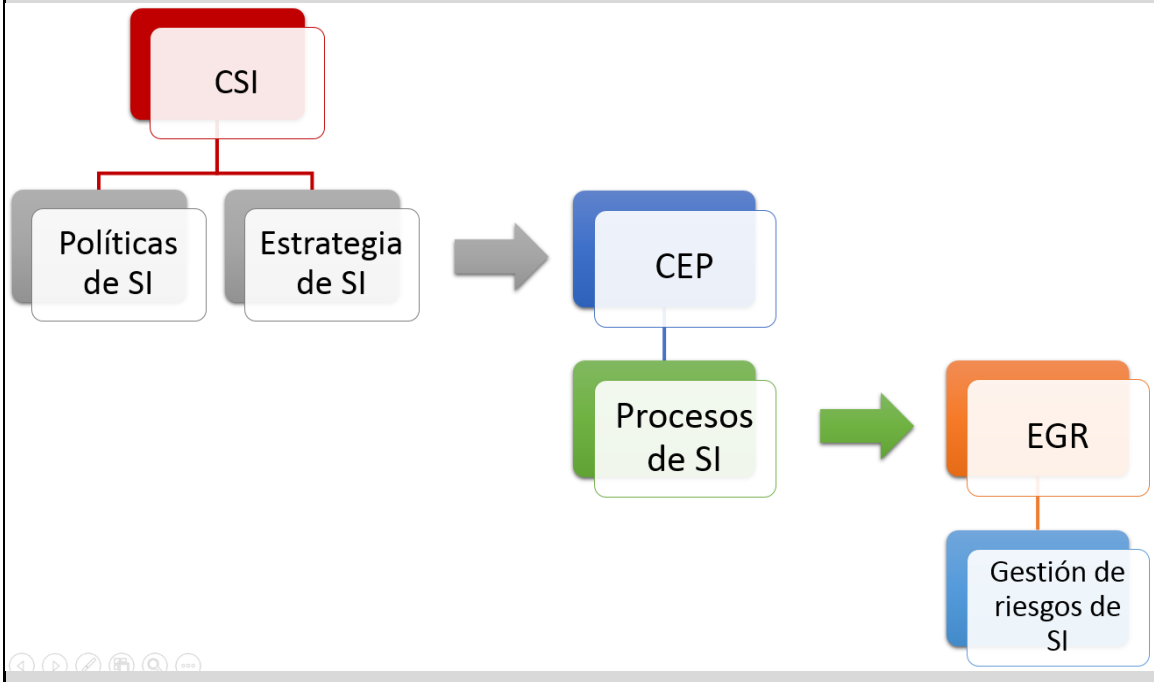
*Los integrantes detallados en c) podrán ser considerados o no miembros permanentes, en función de lo que la organización estime más conveniente.*

*El CEP se reunirá con mayor frecuencia que el CSI, pues su misión es analizar, diseñar, debatir y aprobar nuevos procesos, procedimientos, guías y normas derivadas de las políticas aprobadas por el CSI. En otras palabras, el CEP se encarga de la "bajada a tierra" de los requerimientos de las políticas en procesos, trabaja con la parte táctica y operativa a diferencia del CSI que se encarga del aspecto estratégico de la SI de la organización.*

| LS2.2.4 | Nivel B | F |
|---|---|---|
| Macroproceso de dirección estrategia de la SI<br>Subproceso de establecimiento del CEP | | |
| El CEP debe:<br><br>a) Analizar, diseñar, debatir y aprobar nuevos procesos, procedimientos, guías y normas derivadas de las políticas de SI aprobadas por el CSI.<br>b) Reunirse con las áreas del negocio en las que impactarán los nuevos procesos, procedimientos, guías y normas, con el objetivo de simplificar su implementación y asegurar su alineamiento con las necesidades del negocio.<br>c) Actuar sobre el último eslabón del MRE, realizando la traducción de las políticas a procesos de SI.<br>d) Reunirse regularmente.<br>e) Coordinar las actividades tácticas y operativas de SI de la organización.<br>f) Promover la mejora continua de la SI.<br>g) Monitorear y supervisar el rendimiento operativo de la SI de la organización.<br>h) Gestionar problemas relativos a la privacidad de la información. | | |
| ISF Standard IM1.2.1 [41] | | |

| LS2.2.5 | Nivel B | F |
|---|---|---|
| Subproceso de establecimiento del CEP | | |
| En función del requerimiento LS2.2.3.a, el presidente del CEP:<br><br>a) Es responsable de coordinar las actividades y reuniones del CEP.<br>b) Es responsable del cumplimiento de los requerimientos LS2.2.3 y LS2.2.4. | | |
| LS2.2.2 - LS2.2.3 | | |
| | | |

| LS2.2.6 | Nivel B | F |
|---|---|---|
| Subproceso de establecimiento del CEP<br><br>Subproceso de privacidad de la información | | |
| En función de LS2.2.4.h, el SOO será responsable de coordinar las actividades de la organización vinculadas a la privacidad de la información.<br><br>En función de LS2.2.4.h, el CEP será responsable por:<br><br>a) Estar al tanto de los requerimientos legales, regulatorios y contractuales vinculados a privacidad que la organización debe de cumplir, la localización y forma de almacenamiento de información de identificación personal y como y cuando dicha información es utilizada.<br>b) La implementación y la gestión de un programa de privacidad de la información que incluya la identificación de responsables de privacidad dentro de la organización, la realización de auditorías de cumplimiento de los requerimientos legales, regulatorios y contractuales vinculados a privacidad que la organización debe de cumplir, la realización de actividades de capacitación y toma de conciencia en el marco del PCED y realizar evaluaciones de la privacidad e la información manejada por los procesos y aplicaciones de la organización con el objetivo de identificar riesgos a tratar.<br><br>*El programa detallado en b) deberá de ser diseñado por el CISO y aprobado y establecido por el CSI.* | | |
| LS2.2.2 - LS2.2.3 | | |
| ISF Standard IM1.2.1, IM1.2.2 y IM1.2.3 [41] | | |

| LS2.2.7 | Nivel B | F |
|---|---|---|
| Macroproceso de dirección estrategia de la SI<br>Subproceso de establecimiento del CEP | | |
| La organización deberá de establecer una estructura de gobierno de SI que se adecue a lo establecido en LS2.2.1, LS2.2.2, LS2.2.3, LS2.2.4 y en el presente requerimiento. Dicha estructura deberá diseñarse en forma de cascada según puede visualizarse en la ilustración LS2.2.7.A. | | |
|  | | |
| Ilustración LS2.2.7.A: Estructura modelo de gobierno de SI. | | |
| LS2.2.1 - LS2.2.2 - LS2.2.3 | | |
| ISF Standard SM2.1.2 [41] | | |

[Página dejada en blanco intencionalmente]

## *LS2.3 Gestión de activos de Información*

**Objetivo** Establecer una metodología de clasificación de toda la información de la organización, que se encuentre respaldada por procesos y protocolos que enmarquen todas las actividades de su ciclo de vida a fin de proteger la disponibilidad, integridad y confidencialidad de los AI de la organización [41] [22] [3].

| LS2.3.1 | Nivel E | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de identificación y relevamiento | | |
| Se deberán de identificar todos los AI de la organización y, a su vez, todos aquellos activos vinculados a las instalaciones de procesamiento de información. | | |
| | | |
| ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] - ISF Standard SM1.1.2 [41] | | |

| LS2.3.2 | Nivel E | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de identificación y relevamiento | | |
| Se deben de identificar todos aquellos activos relevantes dentro del ciclo de vida de la información de la organización y, a su vez, documentar su importancia.<br><br>El ciclo de vida de la información deberá de incluir las siguientes etapas:<br><br>a) Creación. | | |

b) Procesamiento.
c) Almacenamiento.
d) Transmisión o en tránsito.
e) Eliminación/destrucción o deterioro.

ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3]

| LS2.3.3 | Nivel E | F |
|---|---|---|

Proceso de gestión de AI

Subproceso de identificación y relevamiento

De la identificación establecida en LS2.3.1, deberá de obtenerse como resultado un mapa de inventario de AI de la organización.

El mapa de inventario de AI deberá de detallar como mínimo de cada AI:

a) RAI responsable por dicho AI.
b) Custodio de dicho AI (en caso de que dicho rol difiera con el RAI).
c) Clasificación de nivel criticidad de dicho AI.
d) Clasificación de nivel confidencialidad, integridad y disponibilidad de dicho AI.
e) Tipo de información.
f) Periodo de validez de la clasificación.

*El mapa de AI deberá de considerar por lo menos los activos intangibles, los activos físicos, activos electrónicos, comunicaciones electrónicas, las instalaciones, la información (hablada, escrita o visualizada) y las personas. A su vez, deberá enumerar ejemplos de tipos de AI para cada nivel de clasificación especificado.*

*Todo AI debe de tener un RAI responsable asignado, los cuales se encargarán de garantizar que los AI a su cargo reciban un apropiado nivel de protección.*

*Se deberá de documentar y proveer una descripción de cada nivel de clasificación establecido en d).*

LS2.3.1

ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3]
– ISF Standard IM1.1.1, IM1.1.2 y IM1.19 [41] –

| LS2.3.4 | Nivel E | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de gestión del inventario de AI | | |
| El mapa de inventario de activos delineado en LS2.3.3 deberá de:<br><br>a) Encontrarse debidamente documentado.<br>b) Ser exacto y consistente.<br>c) Ser actual (deberá de mantenerse actualizado en el tiempo).<br>d) Estar alineado con otros inventarios mantenidos por la organización.<br>e) Ser comunicado y encontrarse disponible. | | |
| | | |
| ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] - ISF Standard SM1.1.8 [41] | | |

| LS2.3.6 | Nivel E | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de clasificación de AI | | |
| Los AI de la organización deberán ser clasificados en función de:<br><br>a) Requerimientos legales, regulatorios, estatutarios, contractuales, de mercado o de SI.<br>b) Valor para la organización.<br>c) Criticidad de la información para la organización.<br>d) Sensibilidad de la confidencialidad de la información.<br>e) Disponibilidad de la información necesaria.<br>f) Nivel de integridad de la información requerido.<br>g) Criticidad de los procesos vinculados a la información.<br>h) La generación o utilización de la información por parte de una AES.<br>i) Impacto en el negocio que generaría la perdida de confidencialidad, disponibilidad y/o integridad de la información.<br><br>La clasificación deberá de ser revisada y actualizada regularmente. A su vez, deberá de ser firmada por el dueño de negocio de dicha información.<br><br>*Se deberán implementar un máximo de 4 niveles de clasificación de confidencialidad, integridad y disponibilidad. En cuanto a criticidad se* | | |

| |
|---|
| *establecerán 4 niveles: BAJA – MEDIA – ALTA – CRITICA. Los AI deben ser protegidos en función de su nivel de criticidad asignado.*<br><br>*El esquema de clasificación deberá de tomar en cuenta todos los requerimientos vinculados a la retención de información (tanto técnicos, como de negocio y legales y reglamentarios).* |
| |
| ISO 27.002 8.1.4 [7] – ISO 27.001 A.8.2.1 [3] - ISF Standard IM1.1.1, SM1.1.2, IM1.1.3 y IM1.1.5 [41] |

| LS2.3.7 | Nivel D | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de identificación y relevamiento | | |
| El mapa de inventario de AI deberá de detallar los siguientes resultados del análisis de riesgo desarrollado por el EGR sobre dicho AI:<br><br>a) Amenazas vinculadas.<br>b) Vulnerabilidades vinculadas.<br>c) Acción o acciones de tratamiento de riesgo.<br>d) Controles delineados vinculados al mismo. | | |
| | | |
| ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] | | |

| LS2.3.8 | Nivel D | K |
|---|---|---|
| Proceso de gestión de AI | | |
| En función de LS1.2.7, la organización deberá de establecer una política de gestión de AI y una política de clasificación de la información que contemple todos los requerimientos correspondientes detallados en los Dominios de SI LS2.3 y LS2.2. | | |
| LS1.2.7 – LS2.3 – LS2.2 | | |
| ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] | | |

| LS2.3.9 | Nivel C | S |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de identificación y relevamiento | | |
| El mapa de inventario de AI deberá de detallar de cada AI:<br><br>a) Procesos de negocio vinculados al mismo.<br>b) Controles asociados al mismo. | | |
| | | |
| ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] | | |

| LS2.3.10 | Nivel C | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de establecimiento de RAI | | |
| El CSI nombrará a un RAI para cada uno de los activos de información identificados en LS2.3.1, en función del requerimiento LS2.3.3.a. | | |
| LS2.3.3.a – LS2.3.3 | | |
| ISO 27.002 8.1.1 y 8.1.2 [7] – ISO 27.001 A.8.1.2 [3] - ISF Standard SM1.1.2 [41] | | |

| LS2.3.11 | Nivel C | K |
|---|---|---|
| Proceso de gestión de AI | | |
| Se deberá diseñar, establecer y mantener el proceso de gestión de activos, el cual deberá de incluir, por lo menos, los siguientes subprocesos:<br><br>a) Proceso de relevamiento de activos de información.<br>b) Proceso de generación del inventario de activos de información.<br>c) Proceso de clasificación de activos de información.<br>d) Proceso de selección y nombramiento de RAI.<br><br>La clasificación de AI deberá de:<br><br>a) Poseer una fecha de efectividad.<br>b) Ser comunicada al custodio del AI. | | |

c) Integrar la realización de las acciones necesarias para que los usuarios conozcan la clasificación y sus revisiones.

*Al finalizar la clasificación de un AI, el RAI deberá de identificar los recursos asociados y los perfiles funcionales que deben tener acceso al mismo.*

*Los detalles de la clasificación de la información deberán de incluirse en los acuerdos que la organización celebre con sus partes interesadas.*

ISO 27.002 8.1.1 [7] – ISO 27.001 A.8.1.1 [3] – ISF Standard SM1.1.8 [41]

| LS2.3.12 | Nivel C | K |
|---|---|---|
| Proceso de gestión de AI<br>Subproceso de clasificación de AI | | |
| Los AI de la organización deberán de ser clasificados en función de lo delineado en LS2.3.6 y las siguientes directivas:<br><br>a) Criticidad de los procesos vinculados a la información.<br>b) La generación o utilización de la información por parte de una AES.<br><br>La clasificación de los AI deberá de encontrarse incluida en los procesos de negocio de la organización.<br><br>*La clasificación deberá de mantenerse actualizada con el objetivo de evitar incurrir en gastos innecesarios (protegiendo información pública o almacenando información obsoleta).* | | |
| LS2.3.6 | | |
| ISO 27.002 8.1.4 [7] – ISO 27.001 A.8.2.1 [3] | | |

| LS2.3.13 | Nivel C | F |
|---|---|---|
| Proceso de gestión de AI<br>Subproceso de clasificación de AI | | |
| El CSI definirá los niveles de clasificación de los AI de la organización. Dichos niveles deberán de incluirse en la Política de Gestión de Activos que el CISO | | |

| |
|---|
| deberá de desarrollar en función de todos los requerimientos detallados en los dominios de SI LS2.2 y LS2.3.<br><br>*Se recomienda que dichos niveles se utilicen de forma general en toda la organización, evitando de esta forma la existencia y probable colisión entre diversos métodos de clasificación de AI en la organización.*<br><br>*Se recomienda que la cantidad de los niveles de clasificación no sea mayor a 4, para evitar que su gestión se torne compleja por parte de los usuarios finales.* |
| LS2.2 – LS2.3 |
| ISO 27.002 8.1.4 [7] – ISO 27.001 A.8.2.1 [3] |

| LS2.3.14 | Nivel C | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de rotulado de información | | |
| Se deben de desarrollar un conjunto apropiado de procesos destinados al rotulado de la información para cada tipo de AI definido en LS2.3.3, en función del esquema de clasificación de la información desarrollado por el CSI (referirse al requerimiento LS2.3.8). | | |
| LS2.3.8 | | |
| ISO 27.002 8.2.2 [7] – ISO 27.001 A.8.2.2 [3] – ISF Standard IM1.1.4 [41] | | |

| LS2.3.15 | Nivel C | K |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de utilización de AI | | |
| Se deben de desarrollar un conjunto apropiado de procesos destinados a la manipulación (manejo, tratamiento, almacenamiento, trasmisión y uso de los AI) de los AI de la organización, en función del esquema de clasificación de la información desarrollado por el CSI (referirse al requerimiento LS2.3.8). | | |
| | | |
| ISO 27.002 8.2.3 [7] – ISO 27.001 A.8.2.3 [3] – ISF Standard IM1.1.4 [41] | | |

| LS2.3.16 | Nivel C | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de adecuación de clasificaciones | | |
| Los acuerdos que incluyan el intercambio de información con otras organizaciones, deberán de incluir procesos para la identificación de la clasificación de dicha información y para interpretar el esquema de clasificación de la información de otras organizaciones.<br><br>*El esquema de clasificación de la organización deberá de proporcionar orientación sobre cómo gestionar las diferencias entre esquemas de clasificación diferentes.* | | |
| | | |
| ISO 27.002 8.2.3 [7] – ISO 27.001 A.8.2.3 [3] | | |

| LS2.3.17 | Nivel C | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de definición de accesos | | |
| Se deberán de definir y documentar los diversos niveles, métodos y formas de autorización de acceso a un cierto AI por parte de un RAI.<br><br>Se debe de establecer un proceso de gestión de autorizaciones habilitación de acceso a información de la organización) por parte de los RAI. El mismo deberá de incluir un subproceso de acreditación y verificación[61] del personal destinatario de dicha autorización.<br><br>Lo realizado por la organización en vías del cumplimiento del presente requerimiento deberá de encontrarse en concordancia con las definiciones del proceso de gestión de accesos definido por en los SSI IS y PD. | | |
| | | |
| | | |

[61] Se establece un proceso de "*clearance*" del personal que accederá a dicho AI. El nivel de rigurosidad de dicho proceso deberá de ser acorde al nivel de SI requerido en función de la naturaleza de la organización.

| LS2.3.18 | Nivel B | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de utilización de AI | | |
| Los procesos detallados en LS2.3.15, deberán de tomar en cuenta los siguientes lineamientos:<br><br>a) Restricciones de acceso que respalden los requisitos de protección para cada nivel de clasificación de la información.<br>b) Mantenimiento de un registro formal destinatarios autorizados de los AI.<br>c) Protección de las copias temporales o permanentes de la información a un nivel compatible con la protección de la información original.<br>d) Almacenamiento de los activos de TI en concordancia con las especificaciones del fabricante.<br>e) Rotulado claro de todas las copias de la información con el objetivo de captar la atención del destinatario autorizado. | | |
| | | |
| ISO 27.002 8.2.3 [7] – ISO 27.001 A.8.2.3 [3] | | |

| LS2.3.19 | Nivel B | F |
|---|---|---|
| Proceso de gestión de AI<br><br>Subproceso de rotulado de información | | |
| Para el desarrollo de los procesos detallados en LS2.3.14, se deberán de tener en cuenta los siguientes lineamientos:<br><br>a) Los procedimientos deberán de alcanzar a la información y a todos los activos vinculados con la misma (sean físicos o electrónicos).<br>b) El rotulado de la información debe ser fácilmente reconocible.<br>c) Los procedimientos deberán dar una guía sobre cómo y dónde implementar el rotulado, en función del mecanismo de acceso a la información y como dichos activos son manejados dependiendo de los tipos de soporte.<br>d) Los procedimientos podrán definir casos donde se omita el rotulado (por ejemplo en el caso de información de carácter público, para reducir la carga de trabajo).<br><br>Todo el personal, contratados y usuarios de terceras partes de la organización deberán conocer y ser conscientes de los procesos de rotulado de la información. | | |

Aquellos procesos de negocio de la organización que generen información, deberán de encontrarse construidos de forma tal que se asegure un correcto rotulado de clasificación de dicha información.

*Se recomienda utilizar etiquetas físicas y metadatos como forma de rotulado de la información.*

*Se debe a su vez tener en cuenta, que ciertas veces el rotulado de la información podría llegar a brindar efectos negativos: los AI clasificados son significativamente más simples de identificar por parte de atacantes, tanto internos como externos.*

ISO 27.002 8.2.2 [7] – ISO 27.001 A.8.2.2 [3]

| LS2.3.20 | Nivel B | F |
|---|---|---|
| Proceso de generación del inventario de SI | | |
| La organización deberá de definir e identificar los activos y procesos de SI y, a su vez, deberá de asignar un responsable para cada activo y proceso identificado.<br><br>La responsabilidad deberá encontrarse claramente documentada. | | |

| LS2.3.21 | Nivel B | F |
|---|---|---|
| Proceso de gestión de AI | | |
| El esquema de clasificación de la organización deberá de proporcionar orientación sobre:<br><br>a) La necesidad de transmitir la clasificación de la información cuando se comparte verbalmente con personas autorizadas.<br>b) Métodos para agregar, reutilizar o readaptar la información (por ejemplo: cambios en el nivel de clasificación). | | |
| ISF Standard IM1.1.4 [41] | | |

| LS2.3.22 | Nivel B | F |
|---|---|---|
| Proceso de gestión de AI | | |
| La clasificación y el rotulado de la información deberá de ser complementado a través del uso de herramientas automatizadas y especializadas que colaborarán en:<br><br>a) El establecimiento de un rotulado simple, rápido y consistente.<br>b) Vincular los detalles de la clasificación de la información a la misma.<br>c) Comuniquen los requerimientos de seguridad y protejan la información. | | |
| | | |
| ISF Standard IM1.1.7 [41] | | |

| LS2.3.23 | Nivel B | F |
|---|---|---|
| Proceso de gestión de AI | | |
| El esquema de clasificación de la organización deberá de ser revisador regularmente con el objetivo de evaluar su efectividad. La revisión de dicho esquema deberá de incluir:<br>a) Capacitaciones y concientizaciones dirigidas a los usuarios del esquema, en función de lecciones aprendidas.<br>b) Monitoreo de la manipulación de la información por parte de los usuarios, con el objetivo de establecer si la misma cumple se realiza en función de los lineamientos del nivel de clasificación correspondiente.<br>c) La revisión de los niveles de calificación establecidos por los usuarios. | | |
| | | |
| ISF Standard IM1.1.10 [41] | | |

| GOB2.3.24 | Nivel A | K |
|---|---|---|
| Proceso de generación del inventario de SI | | |
| Con el objetivo de lograr el uso eficiente de todos los activos vinculados a la SI en toda la organización, se establecerá un inventario de recursos (como anexo al establecido en LS2.3.3) que pueden ser utilizados para reducir costos y añadir valor a través de la SI. Dicho inventario incluirá:<br><br>a) A los especialistas y al personal de SI de la organización.<br>b) Fuentes de conocimiento de SI a lo largo de toda la organización.<br>c) Productos y servicios vinculados a la SI (adquiridos y/o desarrollados). | | |
| | | |
| ISF Standard SG2.2.5 [41] | | |

[Página dejada en blanco intencionalmente]

# 8

# Bibliografía específica

[1] International Organization for Standardization, **ISO/IEC 27.000:2013 Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary**, ISO/IEC, 2013.

[2] International Organization for Standardization, **ISO/IEC 27.001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements**, ISO/IEC, 2005.

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

[4] Elliot Jaques**, La Organización Requerida**, un sistema integrado para crear organizaciones eficaces y aplicar el liderazgo gerencial en el siglo XXI, GRANICA, 2004.

[5] International Organization for Standardization, **ISO 9000 Sistemas de gestión de la calidad – fundamentos y vocabulario**, ISO, 2015.

[6] International Organization for Standardization, **ISO 9001 Sistemas de gestión de la calidad - requisitos**, ISO, 2015.

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

[8] International Organization for Standardization, **IRAM-NM ISO/IEC 27.005:2012 Tecnología de la información – Gestión del riesgo de la seguridad de la inforamción**, IRAM, 2012.

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

[10] International Organization for Standardization, **IRAM-ISO/IEC 27.007 Tecnología de la información – Técnicas de seguridad**, IRAM, 2014.

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

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

[13] Bizagi BPM, **"What is Business Process Management (BPM)?"** https://www.bizagi.com/es/bpm (consultada el 30/06/2017).

[14] Wikipedia, Gestión de Procesos de Negocio, https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_procesos_de_negocio (consultada el 30/06/2017).

[15] Ulrich Kampffmeyer, **ECM: Enterprise Content Management**, PROJECT CONSULT, 2006.

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

[17] Uptime Institute, **TIER Standard: The classification system**, https://uptimeinstitute.com/tiers, (consultada el 30/06/2017).

[18] International Organization for Standardization, **ISO/IEC 27.003 Information technology – Security techniques – Information security system implementation guidance**, ISO/IEC, 2010.

[19] Metodología de Seguridad de la Información de la NSA.

[20] Manuales y guías técnicas de seguridad diseñadas por la NSA.

[21] Manuales y guías de seguridad diseñadas por el Departamento de Seguridad Interior de los EEUU.

[22] ISACA, **COBIT 5 para Seguridad de la Información**, ISACA, 2012

[23] 20 controles críticos para una ciberdefensa efectiva del Instituto SANS

[24] Project Management Institute, **Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK) quinta edición**, PMI, 2013.

[25] Generally Accepted System Security Principles Comittee, **Generally Accepted System Security Principles**, International Information Security Foundation, 2005.

[26] ISO 55.001: estándar internacional sobre el Sistema de Gestión de Activos

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

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

[29] Deaprtment of Standards Malaysia, **MC IEC/ISO 31.010:2011 Risk management - Risk assessment techniques**, DSM, 2011.

[30] ISO 22.301: estándar internacional sobre el Sistema de Gestión de la Continuidad

[31] Raúl Saroka y Mara Irene Misto Macias, **Material brindado durante la cátedra de Gestión Estratégica de la Seguridad Informática dentro de la Especialización en Seguridad Informática de la UBA**, 2017.

[32] British Standard, **25999-1 Business continuity management – code of practice**, BS, 2006.

[33] ANSI, **Estándar ANSI/TIA-942 Telecomunications Infraestructure Standard for Data Centers**, ANSI/TIA, 2005.

[34] International Organization for Standardization, **ISO 27.033 Information Technology - Security Techniques – Network Security**, ISO/IEC, 2015.

[35] DoD, **Directiva de Seguridad de la Información 8570.1 – M**, Departamento de Defensa de los EEUU, 2005.

[36] Capgemini Consultanting, **Information Security Benchmarking 2015**, https://www.slideshare.net/capgemini/information-security-benchmarking-2014, (consultada el 21/08/2017).

[37] Oficina Nacional de Tecnologías de la Información (ONTI), **Política de Seguridad de la Información modelo**, 2015.

[38] Sebastián Pérez Cuesta, **"El desarrollo de la Teoría de la Organización Requerida"** https://es.scribd.com/document/238650746/El-Desarrollo-de-La-Teoria-de-La-Organizacion-Requerida, (consultada el 5/08/2017).

[40] Ministerio de Seguridad de la Nación, **Política de Seguridad de la Información del Ministerio de Seguridad de la Nación**, Ministerio de Seguridad de la Nación, 2015.

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

[42] Wikipedia, Modelo y Notación de Procesos de Negocio, https://es.wikipedia.org/wiki/Business_Process_Model_and_Notation, (consultada el 09/08/2017).

[43] Carnegie Mellon Software Engineering Institute, **OCTAVE®-S Implementation Guide, Version 1.0**, Carnegie Mellon Software Engineering Institute, 2005.

[44] Ministerio del Interior de Finlandia, **Katakri: Information Security audit tools for authorities**, Ministerio del Interior de Finlandia, 2015.

[45] SABSA Institute, **Sherwood Applied Business Security Architecture**, SABSA Institute, 2009.

[46] NIST (National Institute of Standards and Technology), **NIST SP 800-30 Guide for Conducting Risk Assessments**, NIST, 2012.

[47] Global Organization Design Society, **Census of organizations on public record as having used levels of work complexity and human capability at some point**, http://globalro.org/index.php/2010-09-13-08-13-06/organizations-that-use-requisite-organization, (consultada el 31/08/2017).

[48] 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.

[49] Organización para la Cooperación y el Desarrollo Económico (OCDE), **Digital Risk Management fot Economic and Social Prosperity: OECD Recommendation and Companion Document**, OECD Publishing, 2015.

[50] ISACA, ISF & $(ISC)^2$, **Principles for information security practitioners**, ISACA, ISF & $(ISC)^2$, 2010.

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

[Página dejada en blanco intencionalmente]

# 9

# Bibliografía general

Michael Bazzell y Justin Carroll, Mayo 2016, **The Complete Privacy & Security Desk Reference, Volume I: Digital**, ISBN: 9781522778905.

[Página dejada en blanco intencionalmente]

# 10

# Glosario

## *10.1 Nómina de definiciones clave*

**Documentación fuente:** incluye a todos los estándares, normas, marcos teóricos, manuales y guías internacionales, regionales y nacionales de Seguridad de la Información consultadas para la realización del presente trabajo.

**MRU:** Marco de Referencia Unificado en Seguridad de la Información.

**Modelo de Madurez de Seguridad de la Información (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 Seguridad de la Información. Su objetivo es guiar y apoyar a la organización antes, durante y después de la implementación del Sistema de Mejora Continua en Seguridad de la Información.

**Sistema de Mejora Continua en Seguridad de la Información (SMCSI):** implementado por el **MRU**. El mismo contiene todos los requerimientos (controles, buenas prácticas, procesos, procedimientos, etc.) del **MRU**. Se encuentra dividido en 9 grandes Subsistemas de Seguridad de la Información.

**Subsistema de Seguridad de la Información:** conforma los subgrupos en los que los requerimientos del Sistema de Mejora Continua en Seguridad de la Información se encuentran clasificados y organizados.


**Ilustración 10.1.1: componentes del MRU.**

## *10.2 Nómina de definiciones generales*

Acciones correctivas: "*acción realizada para eliminar la causa de una no conformidad y para prevenir la recurrencia*" [1].

AES: Áreas de Extrema Seguridad, establecidas por el MRU.

AI: Activo de Información, conforma cualquier objeto que tenga valor para la organización [41] [1].

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*" [41].

Autenticación: "*la provisión de garantía de que una característica reclamada por una entidad es correcta*" [1].

Autenticidad: "*propiedad que establece que una entidad es quien dice ser*" [1].

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.

**CIPO**[62]**:** 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 Seguridad de la Información. Conforma una de las áreas de Seguridad de la Información requeridas por el SMCSI.

**CISO**[63]**:** Gerente de Seguridad de la Información, 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*" [1], 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*" [22].

**Conformidad:** "cumplimiento de un requisito" [1] del **MRU**.

**Control:** "*medida que modifica riesgo*" [1]. Pueden ser "*procesos, políticas, dispositivos, practicas o cualquier otro tipo de acción que modifica riesgo"* [1].

**CSI:** Comité de Seguridad de la Información, 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

[62] *"Continuous Improvement & Process Office"*, Oficina de Procesos y Mejora Continua por sus siglas en inglés.
[63] "*Chief Information Security Oficer"*, Gerente de Seguridad de la Información por sus siglas en inglés.

incluye al CEO, CFO, COO, CIO, CISO y todos aquellos roles de similares características [12] [1] [22].

**Disponibilidad:** "*propiedad de la información que determina que esta se encuentra accesible y utilizable*" [1] "*de manera confiable y en el momento oportuno" [22] "a petición de una entidad autorizada*" [1].

**EGR:** 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 la misma a corto y largo plazo para las partes interesadas*" [22].

**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 [1] [12].

**Hardware:** "*Cualquier activo físico utilizado para dar soporte a la información o sistemas de la organización*". [41]

**Información documentada:** "*la información que debe de ser controlada y mantenida por una organización y, el medio en el que la misma está contenida*" [1].

**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) [1] [3] [41] [31].

Instalaciones de procesamiento de información: "identifica cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo aloja" [1].

**Integridad:** "*significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio, la autenticidad*" [22], "*la exactitud y la completitud de la información*" [1].

**MRE:** Marco de Referencia del **MRU**. Se detalla en la sección 3.4 del presente trabajo.

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

**No conformidad:** "incumplimiento de un requisito" [1] 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*" [22] 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*" [22].

**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] [1] [49].

**PCED:** Programa de toma de Conciencia, Entrenamiento y Difusión del **MRU**. El mismo se establece dentro del SSI de Recursos Humanos.

**PSI:** Política de Seguridad de la Información.

**RASI:** Responsable de Auditoria de Seguridad de la Información.

**Requerimiento:** medida, control, proceso, política o acción de Seguridad de la Información requerida por el **MRU**.

**RG:** Responsables Gerenciales, todo aquel gerente o titular de un área, división o sección de la organización.

**RMO[64]:** Responsable de Riesgos de Seguridad de la Información de la organización. Conforma una de las áreas de SI requeridas por el SMCSI.

[64] *"Risk Management Office"*, Oficina de Gestión de Riesgos por sus siglas en inglés.

**RP:** 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.

**Seguridad de la Información:** "*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)*" [22]. 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 [1] [3] [41].

**Sistemas de información:** "*aplicaciones, servicios, activos de TI y cualquier otro componente utilizado para manipular información*" [1].

**SMCSI:** Sistema de Mejora Continua en Seguridad de la información.

**SOO[65]:** responsable del día a día de SI, ya que es quien lleva adelante los procesos tácticos y operativos 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 SI requeridas por el SMCSI.

**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" [1].

[65] "*Security Operations Office*", Oficina de Operaciones de Seguridad por sus siglas en inglés.