Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo final de Especialización

Modelado de Procesos de Seguridad de la Información basado en el estándar O-ISM3

Autor:

Oscar Fabián Cardoso Caicedo

Tutor del Trabajo final:

Dr. Juan Pedro Hecht

Año de presentación

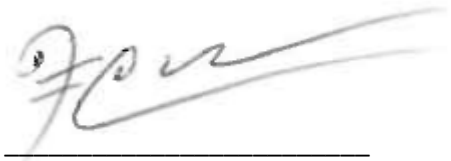
2014

Cohorte

2011

Declaración Jurada de origen de los contenidos

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.



_____

Oscar Fabián Cardoso Caicedo
CC. 14.135.538 Ibagué, Colombia

Resumen

Las áreas de seguridad de la información de las empresas realizan actividades en pro de la protección de sus activos de información, las cuales en muchos casos no disponen de una estructura de procesos asociada, impidiendo de cierta forma tomar las mejores decisiones posibles en beneficio de los objetivos del área y a su vez de la empresa.

La temática propuesta pretende abordar esta necesidad, utilizando como guía estándar el Modelo de Madurez de la Gestión de la Seguridad de la Información O-ISM3[1], donde se establecen procesos por niveles operacionales, tácticos y estratégicos, que permite constituir una visión mucho más global sobre las necesidades reales del área de Seguridad de la información, relacionada directamente al cumplimiento de los objetivos del negocio.

La metodología utilizada para el desarrollo del trabajo será de forma descriptiva, detallando los procesos para cada uno de los niveles, así como las posibles métricas asociadas, la relación existente con otros frameworks o estándares; logrando de esta forma, establecer un modelo de madurez de procesos base que servirá de input para la gestión del área.

Palabras Clave: O-ISM3, activo de información, procesos, objetivos de negocio, métricas, modelo de madurez, Matriz RACI

[1] Open Information Security Management Maturity Model (O-ISM3)

Tabla de contenido

Nómina de Términos y abreviaturas

ISM3 (Information Security Management Maturity Model) [1]: Es un estándar de madurez de seguridad de la información compatible con la implantación de ISO 27001, Cobit, ITIL e ISO 9001, desarrollado por el español Vicente Aceituno.

SGSI [2]: (sistema de Gestión de Seguridad de la información) – La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Activo de información [3]: Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software de sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones , utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de una organización se han de considerar todos los tipos de activos de información.

Proceso [4]: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Métricas [5]: Son herramientas para facilitar la toma de decisiones, mejorar el desempeño y el accountability[2] a través de la colección, análisis y reporte de datos de desempeño relevantes. El propósito de medir el desempeño es monitorear el estado de las actividades medidas y facilitar la mejora de estas aplicando acciones correctivas basadas en medidas observadas.

Modelo de madurez [6]: Los modelos de madurez se utilizan para describir y evaluar el ciclo de vida. El concepto básico de todos los modelos se basa en el hecho de que las cosas cambian con el tiempo y que la mayoría de estos cambios pueden ser predichos o reglamentados.

Matriz RACI [7]: Modelo útil para la asignación de responsabilidades en la ejecución de tareas o actividades asignadas a un proyecto.

[2] Rendición de cuentas de acuerdo al modelo RACI de Cobit

I. Cuerpo Introductorio

1. Introducción

Actualmente las actividades relacionadas a la seguridad de la información tienen como objetivo principal, la protección de los activos considerados como “críticos” para cada organización; dicha valoración dependerá de su objeto de negocio y de la evaluación de riesgos realizada.

Muchas áreas de seguridad que realizan este tipo de actividades trabajan en lograr un nivel de cumplimiento aceptable sobre la confidencialidad, disponibilidad e integridad de la información, sin contar con una guía estándar que permita establecer un enfoque hacia niveles superiores que les genere valor sobre las tareas operacionales que se realizan a diario.

El Modelo de madurez de la gestión de la Seguridad de la información O-ISM3 sirve como guía para cambiar el enfoque técnico y llevarlo a niveles superiores, ya que establece procesos desde niveles operacionales pasando por niveles tácticos hasta llegar a niveles estratégicos, su correcta aplicabilidad servirá de soporte para la asignación de recursos a las áreas de Seguridad. Establecer procesos de seguridad de la información definidos y estandarizados en las organizaciones ayudará a generar controles más específicos y a su vez permitirá cumplir metas y objetivos del área.

2. Objetivos

General

Establecer un enfoque a nivel gerencial sobre los procesos de Seguridad que deberían estar implementados en la mayoría de las organizaciones que disponen de un área de Seguridad de la información.

Específicos

- Relevar información sobre el estándar O-ISM3, métricas de seguridad, Objetivos de Seguridad, nivel de madurez, estándares de seguridad.
- Establecer un modelo gerencial sobre los procesos de seguridad del área de Seguridad de la información, detallando dichos procesos a nivel estratégico, táctico y Operacional.
- Realizar mapeos del estándar O-ISM3 con otros como ISO27002, BCRA 4609, ITIL, etc., de tal forma que permita establecer criterios de comparación sobre los procesos que podrían ser críticos para las organizaciones.
- Establecer un Modelo de madurez base que permita valorar el estado actual de los procesos.
- Proponer métricas que permitan evaluar el desempeño de los procesos.

3. Alcance

Este trabajo se enfocará sobre la aplicabilidad del Modelo de Madurez de la Gestión de la Seguridad de la información (O-ISM3), estableciendo los procesos a nivel estratégico, Táctico y Operativo, sus métricas asociadas, el modelo de madurez para sus procesos y la comparación con otros frameworks o estándares.

II. Cuerpo Principal

1. Estándar ISM3

La gestión de la seguridad de la información en las organizaciones debe estar focalizada sobre la adecuada administración de políticas, procesos métricas y controles de seguridad que permitan mitigar riesgos sobre sus activos de información, de una forma rentable. Es por eso que se exige a las áreas de seguridad actuales, pasar de una visión netamente operativa a una visión más estratégica y gerencial, es decir se debe tener una adecuada gestión de riesgos que permita identificar y estimar niveles de exposición, controles de seguridad para proteger sus activos, y gestión de seguridad que incluyen auditoría y cumplimiento normativo.

El estándar ISM3 se basa en los procesos comunes de seguridad de la información que debería estar implementados y gestionados, además a esto el estándar proporciona:

- Una enfoque por niveles (genérico, estratégico, táctico y operacional), donde en cada nivel se implementan diferentes procesos de seguridad, los cuales pueden ir interrelacionados con otros procesos de otros niveles.
- Sirve como herramienta para la creación de SGSI alineados con la misión de la empresa y el cumplimiento de las necesidades.
- Se aplica a cualquier organización independientemente de su tamaño, el contexto y los recursos.
- Permite a las organizaciones priorizar y optimizar su inversión en seguridad de la información.
- Permite la mejora continua del SGSI estableciendo metas de seguridad y midiendo el desempeño mediante la aplicación de métricas.
- Se adapta a estándares como ISO27001, Cobit, ITIL, Etc, y a normas regulatorias como la 4609 del Banco Central de la República Argentina.

- Sirve como soporte a Auditorías.
- Permite mejorar la gobernabilidad de la organización a nivel tecnológico.

1.1 Modelo ISM3

El modelo de seguridad de ISM3 es adaptable a cualquier tipo de organización, debido a que su metodología se fundamenta en traducir los objetivos del negocio a nivel de seguridad, en especificaciones técnicas de seguridad, tal como se describe en la figura 1. Empezar por conocer las metas corporativas es el primer paso para garantizar la gestión de la seguridad.

Objetivos de negocio: Independiente del objeto de negocio de cada empresa, estas se encargan de fijar metas u objetivos, el logro de cada uno de ellos dependerá de muchos factores que pueden ser críticos o no, uno de estos factores tiene que ver con la seguridad de la información, que puede ser originada por una cultura interna o impuesta por entidades externas como es el caso de la normativa 4609 del Banco Central de la República Argentina. Algunos ejemplos de estas metas u objetivos son:

- Pago de impuestos
- Facturación
- Pago de nomina
- Entrega de productos y/o servicios de excelente calidad
- Mantener registro de todas las operaciones realizadas durante un periodo determinado (para auditorías internas o externas)
- Protección de la propiedad intelectual

Objetivos de Seguridad: ISM3 propone un análisis de dependencia para dar cumplimiento a los objetivos de negocio de la entidad, el objetivo de este

análisis es una lista de objetivos de seguridad como base para el diseño, implementación y monitoreo del SGSI [2]. En otras palabras es poder definir como la seguridad de la información contribuye a la obtención de los objetivos de negocio. Algunos ejemplos de estos objetivos se describen a continuación:

- La facturación solo es accesible al personal de contabilidad
- El sistema registra, nombre de usuario y fecha de quien crea la factura
- La disponibilidad del sistema es acorde al horario laboral
- Existen controles ambientales para proteger el almacenamiento de la información generada por los sistemas.

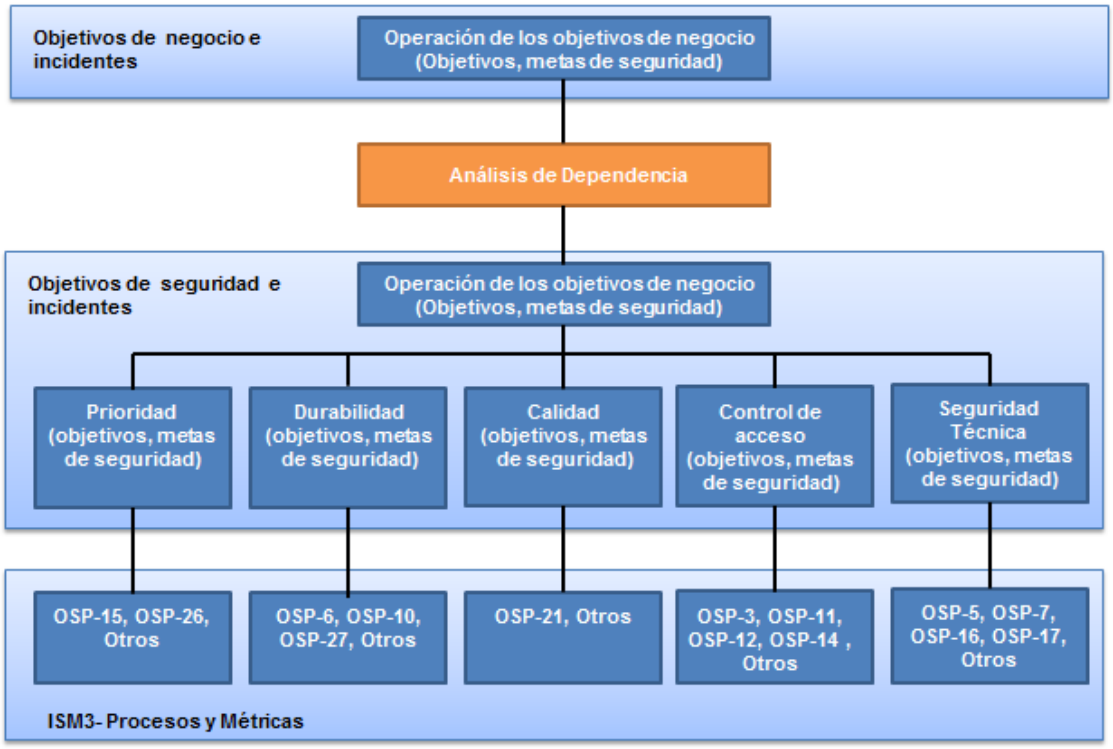


Figura 1 - Modelo ISM3
Fuente: (O-ISM3), Pág. 39.

ISM3 define cinco categorías de objetivos de seguridad:

- Prioridad: Disponibilidad para el negocio, por ejemplo copias de seguridad e identificación de puntos únicos de falla, canales de comunicación e interfaces. Ejemplo:

Prioridad -Objetivos de Seguridad	***Prioridad - Metas de Seguridad***
Disponibilidad: Los repositorios de datos, interfaces o canales de comunicación deben estar disponibles de acuerdo a las necesidades del cliente	8 horas al día, todos los días laborales. La pérdida debe ser inferior al 0.1% del valor contable de la empresa.

- Durabilidad: Integridad de la información, incluyen políticas de mantenimiento planificado y destrucción de la información. Ejemplo:

Durabilidad - Objetivos de Seguridad	***Durabilidad - Metas de Seguridad***
Periodo de retención: el periodo mínimo de un repositorio se mantiene conservado de acuerdo a los requisitos del cliente o requisitos reglamentarios.	Cinco años desde su creación. La pérdida debe ser inferior al 0.1% del valor contable de la empresa

- Calidad de la información: Los objetivos también se refieren a la integridad de la información, técnica de control de calidad que incluyen precisión (o exactitud), relevancia, integridad y consistencia de los repositorios.

Calidad de la información - Objetivos de Seguridad	***Calidad de la información - Metas de Seguridad***
Integridad: Para cumplir o exceder las necesidades del cliente, la información debe ser integra y consistente	El 98% de las Bases de datos deben ser redundantes. La pérdida debe ser inferior al 0.1% del valor contable de la empresa.

- Control de acceso: Requiere la identificación y gestión de los usuarios autorizados. Ejemplo:

Control de Acceso - Objetivos de Seguridad	***Control de Acceso - Metas de Seguridad***
Conceder el uso de servicios, interfaces y acceso a repositorios a personal autorizado	Menos de 25 incidentes por año. La pérdida debe ser inferior al 0.1% del valor contable de la empresa.

- Seguridad Técnica: Generalmente es la infraestructura del Centro de datos como ejemplo tecnología como firewalls, antivirus, parche de seguridad, actualizaciones, el incumplimiento de estos objetivos ponen en situación de riesgos a los demás objetivos de seguridad y del negocio. Ejemplo:

Seguridad Técnica - Objetivos de Seguridad	***Seguridad Técnica - Metas de Seguridad***
Los sistemas ofrecen servicios confiables	el nivel de actualización del antivirus es inferior a un día

Metas de Seguridad: Se definen normalmente en términos de frecuencia de ocurrencia y el umbral de costo de implementación de la misma , teniendo como base el impacto en el negocio, es aquí la importancia de hacer un análisis de dependencia adecuado para soportar la inversión en seguridad.

2. Niveles de Procesos ISM3

El ISM3 proporciona (4) cuatro niveles para la administración de la seguridad de la información:

- Procesos Genéricos (GP): suministra la infraestructura para la implementación, evaluación y mejora de los procesos de gestión de la seguridad de la información.

- Procesos Estratégicos (SSP) – Direcciona y provee: Define los objetivos generales, la coordinación y la provisión de recursos.

- Procesos Tácticos (TSP) – Implementa y Optimiza: Establece el diseño e implementación del SGSI [2], objetivos específicos, y la gestión de los recursos.

- Procesos Operacionales (OSP) – Ejecuta y Reporta: Establece el cumplimento de los objetivos definidos, por medio de procesos técnicos.

A continuación se detalla la gestión de los procesos de seguridad para los diferentes niveles establecidos por el ISM3:

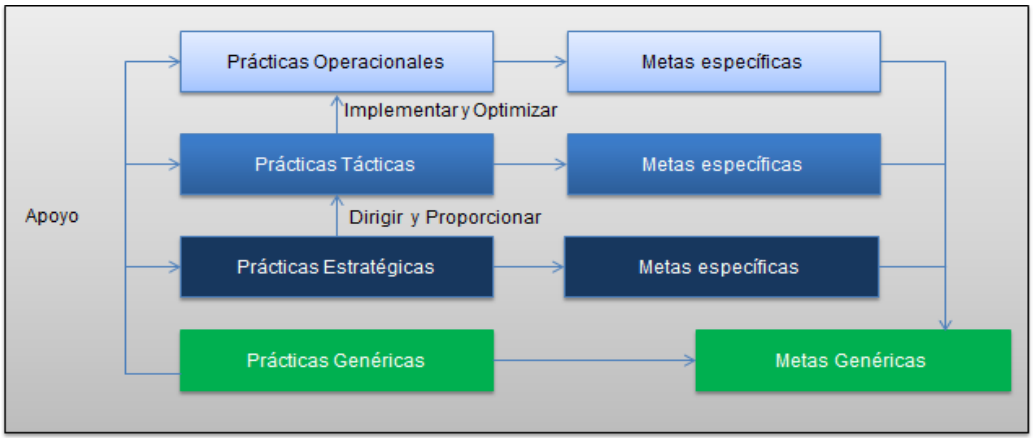


Figura 2 - Gestión de niveles de Seguridad ISM3
Fuente: (O-ISM3), Pág. 51.

El nivel de reporte de gestión de la seguridad de información se detalla en la Figura 3.

Figura 3 - Estructura de reporte
Fuente: (O-ISM3), Pág. 52.

Cada proceso tiene definido una nomenclatura estándar así:

GP -1 Gestión del conocimiento

GP: Identifica que es un proceso genérico
1: Código del proceso
Gestión del conocimiento: Nombre del proceso

2.1 Template para definición de los procesos ISM3

Todo proceso establece entradas, ejecución de actividades y salidas las cuales son el resultado de las actividades realizadas, ISM3 proporciona un témplate estándar para la descripción de cada uno de los procesos, el cual se describe a continuación:

Proceso	Código y Nombre del Proceso
Descripción	Describe las actividades realizadas por el proceso
Valor	Explica los beneficios esperados de este proceso
Documentación	Políticas, procedimientos u otro tipo de normativa que está definida o se requiere definir para mejorar el proceso
Entrada	Entradas para el proceso (por ejemplo lista de procesos que generan entradas a este proceso)
Salida	Resultados del proceso
Descripción de Métricas	Definición apropiada de métricas que permitan evaluar la madurez del proceso

Responsabilidades	Responsable del proceso
Procesos Relacionados	Relación con otros procesos. Algunos profesionales encuentran utilidad en el modelo RACI [7] de cobit para documentar las responsabilidades.
Metodología o herramientas utilizadas	Metodología o mejoras practicas utilizadas para mejorar el proceso

Tabla 1 – Témplate procesos ISM3
Fuente: (O-ISM3), Pág.27.

2.2 Roles y Responsabilidades del proceso

Para que la responsabilidad del proceso sea asumida de una forma correcta, ISM3 propone que la persona o el equipo cuenten con las siguientes capacidades:

Responsabilidad: Tiene un interés personal en obtener un buen resultado para el proceso.

Competencia: Tiene adecuados conocimientos y experiencia

Motivación: Capacidad de Influenciar o generar estímulos hacia el logro de objetivos.

Liderazgo: Tiene la capacidad para tomar decisiones y dar retroalimentación.

Algunos roles relevantes dentro de las organizaciones son descritos a continuación:

- **Stakeholder:** Un accionista, no miembro de la junta ejecutiva, que tiene una participación en el rendimiento de la organización, pero sin participar directamente en la gestión.
- **CEO** o Director General
- **CIO** o Gerente de TI
- **CSO** o Gerente de Seguridad

- **Propietario de proceso:** Responsable de un proceso.
  - **Propietario de sistema**: Responsable de un proceso de negocio que depende de un sistema informático.
  - **Usuario**: Persona autorizada para utilizar un sistema de información.
  - **Oficial de Seguridad de la información**: Gerente de la gestión de la seguridad de la información.
  - **Gerente de unidad de Negocio**: Responsable de la gestión de un segmento de la organización.
  - **Recursos Humanos:** La parte de la organización que selecciona, contrata y administra el personal.
  - **Custodio de datos:** Responsable de la gestión operativa en un repositorio de datos
  - **Administrador de Sistemas**: Responsable con función de administración operacional de un sistema de información.

2.3 Descripción de procesos ISM3

2.3.1 Procesos Genéricos

Son los procesos encargados de proporcionar la infraestructura para la implementación, evaluación y mejora de los procesos del SGSI [2]. Dentro de estos procesos el ISM3 define 3, los cuales se describen a continuación:

2.3.1.1 GP-1 Gestión del Conocimiento

Es el proceso encargado de gestionar el conocimiento dentro de la organización, de acuerdo a ITIL[3]: ***"****El aspecto más beneficioso de trabajar en equipo reside en la oportunidad de compartir el saber, las ideas y la experiencia*

[3] ITIL (Information Technology Infrastructure Library) Estándar aceptado a nivel mundial para la gestión de servicios de TI

acumulada de todos los integrantes del mismo. Este fenómeno se reproduce, a mayor escala, cuando son todos los miembros de una organización los que contribuyen a crear un acervo común de conocimientos.

La experiencia y conocimientos del personal, información de contacto y servicios ofrecidos por los proveedores, así como detalles sobre la rutina diaria (comportamiento de los usuarios, rendimiento de la organización, etc.) constituyen información muy útil para ahorrar tiempo y esfuerzo". [8]

Proceso	**GP-1 - Gestión del Conocimiento**
Descripción	Es encargado de construir, almacenar, comunicar el conocimiento dentro de la organización, de esta manera se obtiene valor sobre la información de la entidad.
Valor	Mejora la eficiencia al reducir la necesidad de volver a adquirir el conocimiento.
Documentación	Normativa asociada a la gestión y mantenimiento del conocimiento adquirido por la empresa.
Entrada	• Conocimiento de expertos • Descripción de procesos, responsabilidades y alcance
Salida	• Políticas, procedimientos, estándares • Listado de documentos (revisados, aprobados, distribuidos) • Reporte de métricas (TSP-4) • Formatos establecidos • Listas de chequeo • Etc.
Descripción de Métricas	• Cantidad de estándares de infraestructura tecnológica de seguridad implementados durante el primer semestre del año.
Responsabilidades	• Dueño del proceso: Responsable de crear o actualizar documentación
Procesos Relacionados	Todos los procesos ISM3
Metodología o herramientas utilizadas	• ITIL • Cobit 5
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A

ISO 27002	N/A
COBIT 5	Dominio BAI - Contruir, Adquirir e implementar Proceso BAI08 – Gestionar el conocimiento
ITIL	Fase Transición del Servicio Proceso - Gestión del conocimiento

2.3.1.2. GP-2 Auditoria del SGSI

Este proceso consiste en validar que las actividades llevadas a cabo por la organización cumplan con los requerimientos internos diseñados para su control, por ejemplo políticas, normas, procesos, procedimientos y a su vez con regulaciones de entidades externas que van a depender del objeto de negocio de la empresa. La o las personas encargadas de auditar el sistema de gestión de la información deberán establecer un método adecuado para la planificación y documentación de la auditoría con el fin de emitir un juicio objetivo e imparcial.

Proceso	**GP-2 - Auditoria del SGSI**
Descripción	Este proceso da soporte para el seguimiento y remediación de las observaciones de auditoría a la seguridad. Este proceso incluye: • Seguimiento de observaciones. • Reporte a la Gerencia de Control Interno y Productividad evidenciando avances sobre observaciones pendientes. • Requerimientos de auditoría (interna, externa) • Pedidos puntuales.
Valor	• Asegurar cumplimiento normativo • Minimizar riesgos futuros
Documentación	Toda la normativa asociada a la protección de activos de información.
Entrada	• Política de seguridad de la información • Documentación de auditoria a los procesos de

	seguridad. • Salidas de cada proceso auditado • Resultados de otras auditorias
Salida	• Reporte de Auditoria • Reporte de métricas
Descripción de Métricas	• % de avance sobre la resolución de observaciones
Responsabilidades	• Supervisor: CEO • Dueño del proceso: Auditores (internos-externos)
Procesos Relacionados	Todos los procesos ISM3
Metodología o herramientas utilizadas	• ISACA – Cobit
Mapeo a otros Frameworks o Normativa	
Normativa 4609	Sección 3.1.4.4. Registros de seguridad y pistas de auditoría.
ISO 27002	15.2.1 Cumplimiento de políticas y estándares de seguridad. 15.2.2 Verificación de cumplimiento técnico. 15.3.1 Controles de auditoría de sistemas de información. 15.3.2 Protección de herramientas de auditoría de sistemas de información.
COBIT 5	Dominio MEA – Supervisar, Evaluar y Valorar • MEA01 – Supervisa, evaluar y valorar rendimiento y conformidad. • MEA02 – Supervisa, evaluar y valorar el sistema de control interno • MEA03 – Supervisa, evaluar y valorar la conformidad con los requerimientos externos
ITIL	N/A

2.3.1.2 GP-3 Diseño y Evolución del sistema de Gestión de la Seguridad (SGSI)

Es el proceso que se encarga de establecer el nivel de Cumplimiento de la organización, seleccionando los procesos operativos más adecuados para alcanzar los objetivos de seguridad. De este análisis dependerá una correcta evaluación porque se deberá conocer los procesos críticos del negocio, la misión de la organización, el cumplimiento regulatorio, protección de datos y de propiedad intelectual.

Proceso	**GP- 3- Diseño y Evolución del SGSI**
Descripción	Valida que los procesos operativos coincidan con las necesidades de la organización y las metas empresariales. El alcance incluye las siguientes áreas: • Misión de la organización • Cumplimiento regulatorio • Protección de la privacidad (empleados – clientes) • Protección de la propiedad intelectual
Valor	Una selección adecuada de los procesos dará un buen retorno de la inversión en seguridad.
Documentación	• Metodología de diseño y evolución del ISM • Política de gestión de riesgos
Entrada	• Política de control del ciclo de vida • Política de seguridad de la información • Metas de seguridad de la información (TSP-3) • Inventario de activos (OSP-3) • Asignación de recursos para la seguridad de la información (SSP-6) • Reportes de incidentes e intrusiones (OSP-24) • Reporte pruebas de backup (OSP-10) • Reporte de pruebas de continuidad de operaciones (OSP-15) • Etc.
Salida	• Amenazas internas y/o externas sobre los objetivos de seguridad
Descripción de	• Conformidad de pruebas realizadas (backup,

Métricas	continuidad) • % de cumplimiento de metas de seguridad
Responsabilidades	• Supervisor: Gerente General y stakeholders representativos • Dueño del proceso: CIO
Procesos Relacionados	• SSP-4 Segregación de funciones • SSP-6 Asignación de recursos para seguridad • TSP-3 Definición de metas de seguridad • TSP-13 Gestión de seguros • OSP-3 Gestión de activos • OSP-19 Auditoria técnica interna • OSP-20 Emulación de incidentes • OSP-24 Gestión de incidentes • OSP-25 Análisis forense informático
Metodología o herramientas utilizadas	• BIA – Evaluación de impacto en el negocio • Evaluación de riesgos: ISO 27005, Magerit, Octave,etc.[4]
Mapeo a otros Frameworks o Normativa	
Normativa 4609	Sección 3 – Protección de activos de información 3.1 Gestión de la Seguridad
ISO 27002	6- Organización de la Seguridad
COBIT 5	Dominio APO – Alinear , Planificar y Organizar APO-13 Gestionar la Seguridad
ITIL	Fase Diseño del Servicio Proceso – Gestión de la seguridad de la información

2.3.2 Procesos de Gestión Estratégica

Son los procesos encargados de establecer un relación costo beneficio, entre el valor que conlleva a la organización la implementación de controles para minimizar el riesgo y el costo que puede ocasionar asumir el riesgo, informando de manera periódica a todos sus stakeholders el estatus del área.

[4] Frameworks utilizados para la evaluación de riesgos

2.3.2.1 SSP-1 Reporte a los Stakeholders

Este proceso establece la realización de los reporte enviados a los stakeholders de acuerdo a la periodicidad previamente definida, demostrando cumplimiento de las regularizaciones aplicables y de las metas de seguridad establecidas.

Proceso	**SSP-1- Reporte a los Stakeholders**
Descripción	Este proceso establece la realización de reportes periódicos a los stakeholders, demostrando el cumplimiento de las regulaciones aplicables y las metas de seguridad.
Valor	Brindar información sobre el desempeño del área, incluyendo desarrollos significativos en seguridad, para la futura toma de decisión sobre inversiones en el área. Brindar información para la gestión de los riesgos operativos
Documentación	Política de protección de activos de información
Entrada	• Reporte Operacional de Seguridad de la Información (OSP-1) • Reporte de Seguridad de Información táctico (TSP-1) • Reportes a la Dirección / Comités (SSP-2 y SSP-4) • Métricas de los restantes procesos estratégicos
Salida	• Reportes de la estrategia de seguridad de la información • Reporte de métricas para los stakeholders
Descripción de Métricas	• Cantidad de reportes presentados a los satkeholders para un periodo de tiempo definido
Responsabilidades	• Supervisor: Stakeholders • Dueño del proceso: CEO y CIO
Procesos Relacionados	TSP-1 Reporte a la gestión estratégica
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	

Normativa 4609	2.1 Comité de Tecnología Informática. Integración y funciones. 2.5.2 Control de gestión.
ISO 27002	6.1.1. Compromiso de la Dirección con la Seguridad de la Información
COBIT 5	Dominio EDM – Evaluar, Orientar, Supervisar EDM-05 Asegurar la transparencia hacia las partes interesadas.
ITIL	N/A

2.3.2.2 SSP- 2 Coordinación

Este proceso establece el modelo de relacionamiento entre los Líderes de la organización y el área de Seguridad informática. Para esto se hace necesario definir comités con las diferentes áreas involucradas por ejemplo comité de sistemas, riesgos, Compliance, documentando en minutas de reunión los temas aquí tratados.

Proceso	**SSP-2- Coordinación**
Descripción	Este proceso establece el modelo de relacionamiento entre los líderes de la organización y el área de Seguridad
Valor	Coordinación entre el personal responsable de la seguridad y líderes de la organización para asegurar el apoyo de todas las áreas y así de esta forma alcanzar los objetivos y optimizar los recursos.
Documentación	Minutas de reunión
Entrada	Seguridad de la información y objetivos de seguridad
Salida	• Minutas de reunión • Métricas de reporte (SSP-1) • Procesos de seguridad de la información que soportan la organización
Descripción de Métricas	• % de participación por área en temas de seguridad (minutas de reunión)

Responsabilidades	• Supervisor: Stakeholders • Dueño del Proceso: CEO
Procesos Relacionados	N/A
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	1 Aspectos Generales 2.4 Dependencia del área de Tecnología Informática y Sistemas. 2.5.1 Planificación 2.5.2 Control de Gestión 3.1.1 Dependencia del área responsable.
ISO 27002	6.1.1. Compromiso de la Dirección con la Seguridad de la Información
COBIT 5	• Dominio EDM – Evaluar, Orientar, Supervisar EDM-04 Asegurar la optimización de los recursos • Dominio APO – Alinear, planificar, organizar APO08 – Gestionar las relaciones
ITIL	N/A

2.3.2.3 SSP- 4 Segregación de Funciones

Este proceso define las reglas para la asignación y gestión de las responsabilidades, contribuyendo así a la reducción de incidentes de seguridad y a su vez ayudando a proteger a la organización contra amenazas internas.

Proceso	**SSP-4- Segregación de Funciones**
Descripción	Este proceso define las reglas para la asignación y gestión de las responsabilidades de seguridad en las áreas técnicas
Valor	Mejorar el uso de recursos y reducir el riesgo de los incidentes de seguridad , ayudando a proteger a la organización de amenazas internas

Documentación	Normativa asociada a la transparencia, asignación, supervisión, rotación y separación de responsabilidades de las personas.
Entrada	Estrategia y objetivos de la organización
Salida	Reportes a los stakeholders (SSP-1)
Descripción de Métricas	N/A
Responsabilidades	Supervisor: Stakeholders Dueño del proceso: CEO y Gerentes de unidades de negocio
Procesos Relacionados	GP-2 Auditoria del SGSI
Metodología o herramientas utilizadas	Matriz RACI
Mapeo a otros Frameworks o Normativa	
Normativa 4609	2.5.3 Segregación de funciones 2.5.4 Actividades y Segregación de funciones. Incompatibilidades 2.5.5 Glosario de funciones descriptas en el cuadro del punto 2.5.4. 3.1.1 Dependencia del área responsable.
ISO 27002	6.1. Estructura para la seguridad de la información 6.1.3 Asignación de responsabilidades 10.1.3 Distribución de funciones
COBIT 5	Dominio APO – Alinear, planificar, organizar APO07- Gestionar los recursos humanos
ITIL	N/A

2.3.2.4 SSP- 6 Asignación de Recursos para la Seguridad de la información

Este proceso asigna recursos para todos los niveles del área de seguridad de la información, las personas, el presupuesto y las instalaciones para la gestión táctica y operativa.

Proceso	SSP-6- Presupuesto para la seguridad de la información
Descripción	Este proceso asigna recursos para seguridad. Incluye la asignación de personas, presupuesto y otros, para todos los niveles de seguridad
Valor	Brindar los recursos necesarios para una gestión adecuada del área.
Documentación	Documentación sobre asignación de recursos, presupuesto, inversiones realizadas, gastos incurridos, etc.
Entrada	• Reporte de valuación de incidentes (TSP-4) • Reporte de ROI y performance del ISM (TSP-4) • Pedidos de recursos de Seguridad de Información (de los procesos tácticos y operacionales)
Salida	• Recursos asignados a la Gestión de la Seguridad de la Información • Presupuesto de Seguridad de la Información (OSP-2) • Reporte de Métricas (SSP-1 y TSP-4)
Descripción de Métricas	• Cantidad de proyectos de inversión presentados, aprobados. • % de Avance en el consumo del presupuesto, tanto de gastos como de inversiones • Cantidad de recursos solicitados vs obtenidos
Responsabilidades	Supervisor: Stakeholders Dueño del proceso: CEO y Gerentes de unidades de negocio
Procesos Relacionados	Todos los procesos ISM
Metodología o herramientas utilizadas	N/A

Mapeo a otros Frameworks o Normativa	
Normativa 4609	1. Aspectos generales 2.5.1 Planificación 3.1.3. Planeamiento de los recursos
ISO 27002	6.1.4 Proceso de autorización de recursos para el tratamiento de la información
COBIT 5	Dominio APO – Alinear, planificar, organizar APO06- Gestionar el presupuesto y los costos
ITIL	Fase – Estrategia del Servicio Proceso – Gestión Financiera

2.3.3 Procesos de Gestión Táctica

La gestión estratégica es el cliente de gestión táctica en relación con los procesos de gestión de seguridad de la información. Es el responsable del uso de los recursos disponibles de la gestión estratégica.

2.3.3.1 TSP-1 Reporte a la Gestión Estratégica

Este proceso genera un reporte de resultados de seguridad sobre el uso de recursos asignados.

Proceso	TSP-1- Reporte a la Gestión Estratégica
Descripción	Este proceso genera un reporte de resultados de seguridad y sobre el uso de los recursos asignados.
Valor	Demostrar a la gestión estratégica la performance, eficiencia y efectividad del modelo.
Documentación	Reporte de seguridad de la información a nivel táctico.
Entrada	• Reporte Operacional de Seguridad de la Información (OSP-1) • Reportes de Métricas de todos los procesos tácticos

	• Reporte de performance y ROI[5] (TSP-4)
Salida	• Reporte de Seguridad de Información táctico (SSP-1)
Descripción de Métricas	• Cantidad de reportes formalizados y acordados • Cantidad de procesos que poseen reportes asociados • Cantidad de métricas de procesos operativos presentadas
Responsabilidades	Supervisor: GP-3 Dueño del proceso Dueño del proceso: CIO o Gerente de seguridad de la información
Procesos Relacionados	OSP-1: Reporte de la Gestión Operacional de la Seguridad
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	2.5.2 Control de gestión.
ISO 27002	6.1.1. Compromiso de la Dirección con la Seguridad de la Información • respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización
COBIT 5	Dominio APO – Alinear , Planificar y Organizar APO-13 Gestionar la Seguridad
ITIL	Fase Diseño del Servicio Proceso – Gestión de la seguridad de la información

2.3.3.2 TSP-2 Administración de Recursos Asignados

En este proceso se asignan todos los recursos a nivel táctico y operativo.

[5] Retorno de la Inversión

Proceso	TSP-2- Administración de Recursos Asignados
Descripción	La gestión nivel táctico asigna los recursos a todos los procesos de gestión táctica y operativa
Valor	Planificación y control en la asignación de recursos para garantizar que el ISM está configurado para alcanzar los objetivos de seguridad.
Documentación	• Registro de solicitudes de requerimientos de recursos para seguridad de la información • Registro de asignación de recursos para seguridad de la información
Entrada	• Información del presupuesto de seguridad SSP-6 • Solicitud de recursos para la seguridad de la información (procesos tácticos y operativos)
Salida	• Asignación de recursos para la seguridad de la información (procesos tácticos y operativos) • Reporte de métricas TSP-4
Descripción de Métricas	• % de recursos asignado a procesos tácticos • % de recursos asignado a procesos operativos
Responsabilidades	Supervisor: GP-3 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	SSP-6 Asignación de recursos para la seguridad de la información
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	1. Aspectos generales 2.5.1 Planificación 3.1.3. Planeamiento de los recursos
ISO 27002	6.1.4 Proceso de autorización de recursos para el tratamiento de la información
COBIT 5	Dominio APO – Alinear, planificar, organizar APO06- Gestionar el presupuesto y los costos
ITIL	Fase – Estrategia del Servicio Proceso – Gestión Financiera

2.3.3.3 TSP-3 Definición de metas y objetivos de Seguridad

Este proceso establece metas de seguridad para objetivos de negocio específicos, para dominios de TI asociados, estándares y políticas relacionadas.

Proceso	**TSP-3- Definición de metas y objetivos de seguridad**
Descripción	Este proceso establece metas de seguridad para objetivos de negocio específicos, objetivos de seguridad para los dominios de IT asociados y estándares y políticas relacionados.
Valor	Proveer las bases para construir los procesos del modelo SGSI
Documentación	• Objetivos de seguridad de la información • Requisitos de clasificación de la información
Entrada	• Política de seguridad de la información
Salida	• Objetivos y metas de seguridad • Documentación de los requisitos de clasificación de la información • Aceptación de uso de la política • Reporte de métricas (TSP-4)
Descripción de Métricas	N/A
Responsabilidades	Supervisor: GP-3 Dueño del proceso Dueño del proceso: CIO
Procesos Relacionados	GP- 3- Diseño y Evolución del SGSI
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	Sección 3 – Protección de activos de información 3.1 Gestión de la Seguridad
ISO 27002	5- Política de seguridad 6- Organización de la Seguridad
COBIT 5	Dominio APO – Alinear , Planificar y Organizar APO-13 Gestionar la Seguridad

ITIL	Fase Diseño del Servicio Proceso – Gestión de la seguridad de la información

2.3.3.4 TSP-4 Gestión de Niveles de Servicio

Este proceso es encargado de gestionar los SLAs[6]. De acuerdo a ITIL: "*responsable de acordar y garantizar los niveles de calidad de los servicios TI prestados".* Como tarea principal esta establecer las métricas de los procesos del modelo.

Proceso	**TSP-4- Gestión de Niveles de Servicio**
Descripción	Este proceso define las métricas de los procesos del modelo.
Valor	• Provee las métricas necesarias para gestionar adecuadamente el área. • Brinda una herramienta de control.
Documentación	• Definición de métricas para cada proceso • Reporte de incidentes • Reporte de rendimiento y retorno de la inversión
Entrada	• Objetivos de Seguridad de la Información (TSP-3) • Registro de condiciones ambientales (OSP-14). • Reporte de Concientización en Seguridad (TSP-11) • Logs de registración denegada.(OSP-12) • Reporte de intentos de accesos no autorizados (OSP-11) • Reporte diario del nivel de actualización y protección ante la propagación de código malicioso (OSP-17). • Reporte de métricas (OSP-17). • Reportes de intrusiones (OSP-24) • Informe forense informático (OSP-25) • Reportes de Métricas de todos los procesos operacionales

[6] SLA (Service Level Agreement) – Acuerdos de niveles de servicio

Salida	• Remediaciones de errores y fallos en los procesos: • Definición de las métricas de los procesos (para todos los procesos operacionales) • Reporte de valuación de incidentes (SSP-6) • Reporte de performance y ROI (TSP-1, SSP-6) • Reportes de Métricas (TSP-1)
Descripción de Métricas	• Cantidad de SLAs definidos • Cantidad de métricas obtenidas
Responsabilidades	Supervisor: GP-3 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	TSP-3: Definición de objetivos y metas de seguridad OSP-24: Manejo de Incidentes y Vulnerabilidades OSP-25: Análisis Forense informático
Metodología o herramientas utilizadas	ITIL
Mapeo a otros Frameworks o Normativa	
Normativa 4609	7.6 control de actividades delegadas
ISO 27002	• 6.1.5. Acuerdos de Confidencialidad • 6.2.2 Tratamiento de la seguridad en la relación con los clientes • 6.2.3 Tratamiento de la seguridad en contratos con terceros • 10.2.1. Prestación de servicios • 10. 8. 2. Acuerdos de intercambio
COBIT 5	N/A
ITIL	Fase Diseño del servicio Proceso Gestión de niveles de servicio

2.3.3.5 TSP-6 Arquitectura de Seguridad

El proceso logra tener una definición clara sobre la arquitectura de seguridad de TI, de tal forma que se pueda aplicar soluciones escalables para la creación y evolución de nuevos sistemas de información que sirvan a la organización.

Proceso	TSP-6- Arquitectura de seguridad
Descripción	Este proceso logra: La arquitectura de seguridad de TI de la organización, el uso de patrones de seguridad para ofrecer soluciones genéricas y escalables.
Valor	La implementación de patrones de seguridad reduce los costos y los riesgos, y aumenta la agilidad en la implementación de sistemas de información.
Documentación	Arquitectura de seguridad
Entrada	Política control del ciclo de vida sistemas de información
Salida	• Definición de dominios y ciclo de vida de TI • Reporte de métricas TSP-4
Descripción de Métricas	N/A
Responsabilidades	Dueño del Proceso: CIO
Procesos Relacionados	OSP-4 Seguridad en control de cambios
Metodología o herramientas utilizadas	TOGAF 9
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	12.1 Requisitos de seguridad de los sistemas
COBIT 5	Catalizador: Servicios, infraestructura y aplicaciones
ITIL	ITIL Proporciona un guía para el diseño y operación de los servicios.

2.3.3.6 TSP-13 Gestión de Seguros

Este proceso utiliza seguros para transferir el riesgo a un tercero a cambio del pago de una tasa fija.

Proceso	TSP-13- Gestión de Seguros
Descripción	Esta medida utiliza seguros para transferir el riesgo a un tercero, a cambio del pago de una tasa fija.
Valor	Mitigar el impacto financiero de riesgos de seguridad que no pueden ser controlados por la entidad, a través de la suscripción de una póliza de seguro adecuada.
Documentación	Política de gestión de riesgos
Entrada	Inventario de activos OSP-3
Salida	• Contrato de Seguros OPS-15 • Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de seguros adquiridos
Responsabilidades	Supervisor: GP-3 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	GP- 3- Diseño y Evolución del SGSI
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	N/A
COBIT 5	N/A
ITIL	N/A

2.3.3.7 TSP-7 Revisión de Antecedentes

Este proceso tiene como objetivo asegurar que los nuevos empleados en puestos sensibles no suponen una amenaza para la organización.

Proceso	TSP-7- Revisión de antecedentes
Descripción	Este proceso tiene como objetivo asegurar que los nuevos empleados no sean una amenaza para la organización
Valor	Las verificaciones de antecedentes se pueden utilizar para evaluar la idoneidad de los

	potenciales empleados
Documentación	Procedimiento de revisión de antecedents
Entrada	• Política de Recursos Humanos • Definición de puestos de trabajo
Salida	• Reporte de revisión de antecedentes (RRHH) • Reporte de métricas TSP-4
Descripción de Métricas	N/A
Responsabilidades	Supervisor: Dueño de proceso GP-3 Dueño del proceso: Recursos Humanos
Procesos Relacionados	TSP-8 Personal de seguridad
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	8.1.2 Selección
COBIT 5	Dominio APO APO07 Gestionar los recursos humanos
ITIL	N/A

2.3.3.8 TSP-8 Gestión de Personal de Seguridad

Este proceso tiene como objetivo asegurar que los empleados relacionados con la seguridad sean confiables y tengas las capacidades y habilidades necesarias para cubrir su función.

Proceso	**TSP-8- Gestión de personal de seguridad**
Descripción	Este proceso tiene como objetivo asegurar el compromiso, capacidad, conocimiento y experiencia de los empleados, Este proceso está estrechamente vinculado con el proceso OSP-12, de modo que los cambios de rol personal se reflejan de inmediato sobre los derechos de acceso, que este posea.
Valor	Establecer la competencia del personal de

	seguridad, mediante entrevistas de selección, certificaciones profesionales y títulos académicos.
Documentación	Procedimiento de selección de personal
Entrada	• Definición de puestos de trabajo • Política de Recursos Humanos • Contratos • Esquemas de desarrollo a nivel personal y profesional
Salida	• Reporte de selección de personal • Rotación de personal OSP-12 • Reporte de métricas TSP-4
Descripción de Métricas	• Cantidad de persona contratadas por periodo establecido
Responsabilidades	Supervisor: Dueño de proceso GP-3 Dueño del proceso: Recursos Humanos
Procesos Relacionados	TSP-7 Revisión de antecedentes
Metodología o herramientas utilizadas	Marco de competencias para la era de la información (SFIA-Skills Framework for the Information Age)[7]
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	8. Seguridad de los Recursos Humanos 8.1.2 Selección 8.1.3 Términos y condiciones laborales
COBIT 5	Dominio APO APO07 Gestionar los recursos humanos Catalizador 5 personas, habilidades y competencias
ITIL	N/A

2.3.3.9 TSP-9 Entrenamiento del Personal de Seguridad

Este proceso asegura que el personal de seguridad desarrolle sus habilidades y competencias profesionales

[7] *www.sfia.org.uk*

Proceso	TSP-9- Entrenamiento de personal de seguridad
Descripción	Este proceso asegura que el personal de seguridad desarrolle sus habilidades y competencias.
Valor	Se requiere un programa de capacitación y desarrollo planificado y monitoreado para asegurar que los procesos se llevan a cabo por personal competente.
Documentación	• Plan de entrenamiento de personal de seguridad • Reporte de entrenamiento en temas de seguridad
Entrada	Política de Recursos Humanos
Salida	• Reporte de entrenamiento en temas de seguridad (Recursos Humanos) • Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de personal capacitado por periodo de tiempo
Responsabilidades	Supervisor: Dueño de proceso GP-3 Dueño del proceso: Recursos Humanos
Procesos Relacionados	N/A
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	8.2.2 Educación, formación y concientización sobre la seguridad de la información
COBIT 5	Dominio APO APO07 Gestionar los recursos humanos Catalizador 5 personas, habilidades y competencias
ITIL	N/A

2.3.3.10 TSP-10 Procesos Disciplinarios

Los procedimientos disciplinarios ayudan a prevenir y mitigar incidentes resultantes de la mala conducta de los empleados.

Proceso	TSP-10- Procesos Disciplinarios
Descripción	Los procedimientos disciplinarios permite prevenir y mitigar los incidentes resultantes de la mala conducta de los empleados.
Valor	Establecer un proceso disciplinario permite hacer cumplir las responsabilidades de los empleados a nivel de seguridad.
Documentación	Procedimiento disciplinario
Entrada	• Reporte de incidentes OSP-24 • Contracto de empleados RRHH • Aceptación de la política de seguridad TSP-3
Salida	Reportes disciplinarios RRHH Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de conductas fraudulentas en un periodo establecido
Responsabilidades	Supervisor: Dueño de proceso GP-3 Dueño del proceso: Recursos Humanos
Procesos Relacionados	N/A
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	8. Seguridad de los Recursos Humanos 8.2.3 Proceso Disciplinario
COBIT 5	N/A
ITIL	N/A

2.3.3.11 TSP-11 Concientización en Seguridad

Este proceso informa y educa a todos los usuarios de la organización sobre la importancia de la seguridad de la información.

Proceso	TSP-11- Concientización en Seguridad
Descripción	Este proceso informa y educa a todos los usuarios de la organización sobre la importancia de la seguridad de la información.
Valor	Un estándar alto de conciencia de la seguridad a través de toda la organización es requerido para prevenir y mitigar incidentes de seguridad. Reforzar el cuidado del activo más importante para la organización, La Información.
Documentación	Reportes de concientización en temas de seguridad
Entrada	• Política de seguridad de la información • Aceptación de la política de seguridad de la información TSP-3
Salida	• Reporte de concientización en temas de seguridad TSP-4 • Reporte de métricas TSP-4
Descripción de Métricas	• % Cumplimiento de la ejecución del Plan de Concientización • Cantidad de temas de concientización "comunicados" en un periodo de tiempo establecido
Responsabilidades	Supervisor: Dueño de proceso GP-3 Dueño del proceso: Recursos Humanos
Procesos Relacionados	N/A
Metodología o herramientas utilizadas	Envío de mails, campañas de comunicación y difusión, capacitación, etc.
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.5 Responsabilidades del área. La instrucción y el entrenamiento en materia de seguridad de la información.
ISO 27002	8. Seguridad de los Recursos Humanos 8.2.2 Educación, formación y concientización sobre la seguridad de la información
COBIT 5	N/A
ITIL	N/A

2.3.3.12 TSP-14 Información de las Operaciones

Este proceso permite obtener información sobre las capacidades de los atacantes potenciales e informa sobre las fortalezas y debilidades de la organización.

Proceso	TSP-14- Información de operaciones
Descripción	Este proceso permite obtener información sobre las capacidades de los atacantes potenciales e informa sobre las fortalezas y debilidades de la organización.
Valor	Obtener información completa y precisa sobre los atacantes potenciales, aumenta la probabilidad de que la organización esté mejor protegida.
Documentación	• Política de seguridad de la información • Reporte de capacidades de posibles atacantes
Entrada	• Política de seguridad de la información • Test de vulnerabilidades
Salida	Reporte de espionaje de potenciales atacantes
Descripción de Métricas	Cantidad de incidentes evitados por posibles atacantes potenciales
Responsabilidades	• Supervisor: GP-3 Dueño del proceso • Dueño del proceso: Gerente de Seguridad de la información
Procesos Relacionados	N/A
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	N/A
COBIT 5	N/A
ITIL	N/A

2.3.4 Procesos de Gestión Operacional

La gestión operacional reporta al CIO (Gerente de TI) y al Gerente de seguridad de la información (gestión Táctica). Ver Figura [X] Estructura de Reporte.

2.3.4.1 OSP-1 Reporte de la Gestión Operacional de seguridad

Proceso que permite emitir un reporte de los resultados de los procesos operativos y de los recursos alocados.

Proceso	**OSP-1- Reporte de la Gestión Operacional de Seguridad**
Descripción	Reporte regular de los resultados de los procesos operativos y del uso de los recursos alocados.
Valor	Este tipo de reportes para la gestión táctica permite mostrar el desempeño y efectividad de los procesos.
Documentación	Reporte de procesos operacionales
Entrada	Reporte de métricas de procesos operacionales
Salida	Reporte operacional de seguridad de la información
Descripción de Métricas	• Ranking de procesos con fallas detectadas • % de Incidentes con criticidad Alta • % de Incidentes que ocurrieron por falla en los controles • % de Incidentes no anticipados en el análisis de riesgos • % de observaciones de Auditoria calificadas como “aceptables” • % de observaciones Auditoria que ocurrieron por falla en los controles • % de observaciones Auditoria calificadas con riesgo Alto no anticipadas en el análisis de riesgos
Responsabilidades	Supervisor: TSP-14 Dueño del Proceso Dueño del proceso: Gerente de seguridad informática
Procesos	OSP-3 Gestión de activos

Relacionados	OSP-20 Emulación de incidentes OSP-23 Detección y análisis de eventos internos OSP-24 Gestión de incidentes
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.5. Responsabilidades del área. Los controles efectuados por el área deben establecerse formalmente a través de reportes operativos, que permitan la supervisión continua y directa de las tareas y el análisis del logro de las metas definidas.
ISO 27002	N/A
COBIT 5	N/A
ITIL	N/A

2.3.4.2 OSP-2 Adquisición en Seguridad

Proceso encargado de la selección de proveedores y/o productos y servicios específicos de seguridad que mejor cumplan con los objetivos de seguridad de la información y las métricas dentro del presupuesto asignado.

Proceso	**OSP-2- Adquisición en Seguridad**
Descripción	Selección de proveedores y productos/servicios específicos de seguridad que mejor cumplan los objetivos de seguridad de la información y las métricas dentro del presupuesto asignado.
Valor	Permite hacer un uso más eficiente de los recursos.
Documentación	Reporte de recomendaciones de adquisición
Entrada	SSP 6 - Presupuesto para la seguridad de la información TSP 3 – Metas y objetivos de seguridad de la información

Salida	Recomendaciones de compras Reporte de métricas TSP-4
Descripción de Métricas	• Número de incidentes de seguridad causados por la selección de proveedores y productos/servicios que no cumplieron con los objetivos fijados. • Porcentaje de proveedores con los cuales se ha establecido un acuerdo de nivel de servicio.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de Seguridad de la información
Procesos Relacionados	GP-3 Diseño y evolución del SGSI
Metodología o herramientas utilizadas	ISO/IEC 15408:2009
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.3. Planeamiento de los recursos. 7.3. Formalización de la delegación. 7.5. Implementación del procesamiento de datos en un tercero.
ISO 27002	6.2.1 Identificación de los riesgos relacionados con las partes externas 6.2.2 Consideraciones de la seguridad cuando se trata con los clientes 6.2.3 Consideraciones de seguridad en los acuerdos con terceras partes
COBIT 5	Dominio APO Alinear, Planificar y Organizar APO10 Gestionar los proveedores
ITIL	Fase Diseño del Servicio Proceso Gestión de proveedores

2.3.4.3 OSP-3 Gestión de inventario de activos de información

En este proceso se identifica al dueño de cada activo de información, al proceso al que pertenece el activo, el estado actual y las dependencias del mismo respecto a otros activos.

Proceso	**OSP-3- Gestión de inventario de activos de información**
Descripción	Este proceso identifica los activos a ser protegidos

Valor	Identificación de los activos críticos a proteger y su grado de utilización.
Documentación	• Procedimiento de inventario de activos • Procedimiento de nombramiento y etiquetado de activos • Clasificación y requisitos de información
Entrada	Inventario de Hardware Inventario de Software Otros repositorios de información
Salida	Inventario de Activos Reporte de métricas TSP-4
Descripción de Métricas	• % de procesos de negocio en el inventario. • % de procesos de soporte en el inventario. • % de aplicaciones en el inventario. • % de tipos de activos en el inventario.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de TI
Procesos Relacionados	TSP-3 Metas y objetivos de Seguridad OSP-4 Seguridad en la gestión de cambios
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.2 Inventario Tecnológico
ISO 27002	7.1.1 Inventario de activos 7.1.2 Propiedad de los activos. 7.2.1 Guías de clasificación.
COBIT 5	Dominio BAI construir, Adquirir e Implementar BAI09 Gestionar los activos
ITIL	Fase Transición del Servicio Proceso Gestión de la configuración y activos del servicio

2.3.4.4 OSP-4 Seguridad en la Gestión de Cambios

Este proceso previene incidentes de cambios en el estado de medidas de seguridad en un activo de TI.

Proceso	OSP-4- Seguridad en la Gestión de Cambios
Descripción	Este proceso previene incidentes relacionados a cambios en el estado de medidas de seguridad en un activo de TI.
Valor	Evitar incidentes y cambios no autorizados que pueden resultar de un proceso de cambios poco formal.
Documentación	• Política del control de cambios • Procedimiento de cambios a componentes de seguridad
Entrada	OSP-5 Actualizaciones de seguridad OSP-6 Depuración y /o Destrucción de activos OSP-7 Securitización de activos OSP-19 Auditoria técnica interna OSP-21Calidad de información y evaluación de cumplimiento OSP-22 Monitoreo de alertas
Salida	• Minuta con el detalle de cambios aceptados y rechazados. • Implementación del cambio.
Descripción de Métricas	• Porcentaje de cambios en los que se detectaron vulnerabilidades de seguridad. • Porcentaje de cambios no autorizados por vulnerabilidades de seguridad.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del Proceso : Gerente de seguridad de la información
Procesos Relacionados	OSP-5 Actualizaciones de seguridad OSP-6 Depuración y /o Destrucción de activos OSP-7 Securitización de activos OSP-22 Monitoreo de alertas
Metodología o herramientas utilizadas	Herramientas para el análisis de seguridad de software
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.8. Control de cambios a los sistemas productivos.
ISO 27002	10.1 Procedimientos y responsabilidades operacionales. 10.1.2 Gestión de cambios. 10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación 12.5.1 Procedimientos de control de cambios. 12.5.2 Revisión técnica de los cambios en el sistema operativo.

COBIT 5	Dominio BAI Construir , Adquirir e implementar BAI06 Gestionar los cambios
ITIL	Fase Transición del servicio Proceso Gestión de cambios

2.3.4.5 OSP-5 Actualizaciones de Seguridad

Este proceso controla la actualización de los sistemas y aplicativos, a fin de prevenir incidentes y/o la explotación de vulnerabilidades.

Proceso	**OSP-5- Actualizaciones de Seguridad**
Descripción	Este proceso controla la actualización de los sistemas y aplicativos, a fin de prevenir incidentes y/o la explotación de vulnerabilidades.
Valor	La actualización de parches de seguridad evita incidentes derivados de la explotación de las debilidades conocidas de los sistemas y aplicativos.
Documentación	Procedimiento de gestión de parches
Entrada	OSP-3 Inventario de activos
Salida	• Reporte del nivel de actualización de los sistemas y aplicaciones. • TSP 4 - Reporte de métricas
Descripción de Métricas	• Cantidad de parches de seguridad que se implementaron para hacer frente a las vulnerabilidades identificadas. • Número de parches de seguridad pendientes de implementación, por criticidad y tipo de tecnología. • Nivel general de actualización de la red.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de Operaciones de TI
Procesos Relacionados	OSP-4 Gestión de cambios OSP-9 Medidas de seguridad de control de cambios
Metodología o herramientas utilizadas	

Mapeo a otros Frameworks o Normativa	
Normativa 4609	
ISO 27002	12.5 Seguridad en los procesos de desarrollo y soporte. 12.5.1 Procedimientos de control de cambios. 12.5.2 Revisión técnica de las aplicaciones después de los cambios al sistema operativo. 12.5.3 Restricciones en los cambios a los paquetes de software. 12.6.1 Control de vulnerabilidades técnicas
COBIT 5	Dominio DSS Entregar, Dar servicio y Soporte DSS01 – Gestionar las operaciones
ITIL	Fase Operación del Servicio Función Gestión de Operaciones de TI

2.3.4.6 OSP-6 Depuración y/o Destrucción de Activos de Información

Este proceso cubre procedimientos para depurar activos o parte de ellos a ser reemplazados, como así también procedimientos para su destrucción con el fin de prevenir la revelación de información sensible.

Proceso	**OSP-6- Depuración y/o Destrucción de Activos de Información**
Descripción	Este proceso cubre procedimientos para depurar activos o parte de ellos a ser reemplazados, como así también procedimientos para su destrucción con el fin de prevenir la revelación de información sensible.
Valor	• Prevención de incidentes ocurridos por mantener el acceso a información sensible en desuso. • Evitar que información en medios como cintas o discos quede expuesta al salir de un dominio de TI o al pasar fuera del control de la organización
Documentación	Reporte de activos dados de baja
Entrada	Inventario de activos OSP-03

Salida	Confirmación formal del borrado o destrucción de repositorios y/o de los medios o equipos que los soportan.
Descripción de Métricas	• Porcentaje de activos dados de baja del inventario y que cuentan con confirmación formal de borrado o destrucción. • Tiempo de respuesta promedio ante requerimientos de depuración de activos.
Responsabilidades	Supervisor: TSP-14 Dueño de proceso Dueño de proceso: Gerente de TI
Procesos Relacionados	OSP-3 Gestión de activos OSP-4 Gestión de cambios OSP-9 Medidas de seguridad de control de cambios OSP-27 Gestión de archivo
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.2.4. Destrucción de residuos y de medios de almacenamiento de información.
ISO 27002	9.2.6 Seguridad en la reutilización o eliminación de equipos. 10.7.2 Eliminación de medios.
COBIT 5	N/A
ITIL	N/A

2.3.4.7 OSP-7 Securitización de Activos

Este proceso mejora la configuración de seguridad a nivel de canales, servicios, puertos, interfaces y repositorios, mejorando de esta forma su confiabilidad.

Proceso	**OSP-7- Securitización de activos**
Descripción	Este proceso mejora la configuración de canales, servicios, puertos, interfaces, y repositorios; mejorando su confiabilidad.
Valor	La securitización contribuye a proteger la

	confidencialidad, disponibilidad e integridad de la información.
Documentación	Procedimiento de securización de servicios Procedimiento de securización de canales Procedimiento de securización de interfaces Procedimiento de securización de repositorios
Entrada	Inventario de activos
Salida	Seguridad de servicios, canales, puertos, interfaces, repositorios
Descripción de Métricas	• Número de activos de TI con requerimientos de seguridad pendientes. • Porcentaje de activos de TI con requerimientos de seguridad pendientes. • Número de activos de TI conteniendo información sensible con requerimientos de seguridad pendientes. • Porcentaje de activos de TI conteniendo información sensible con requerimientos de seguridad pendientes. • Número de medidas de seguridad implementadas que solucionan incidentes/vulnerabilidades de seguridad identificadas.
Responsabilidades	Supervisor: TSP-14 Dueño de proceso Dueño de proceso: Gerente de TI
Procesos Relacionados	OSP-4 Gestión de cambios OSP-9 Medidas de seguridad de control de cambios
Metodología o herramientas utilizadas	Sistemas de encripción
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.4.4. Registros de seguridad y pistas de auditoría. 6.4. Operatoria y control de las transacciones cursadas por medio de Internet (e-banking).
ISO 27002	10.3.2 Aceptación del sistema. • Existencia de un conjunto acordado de controles y medidas de seguridad instaladas según el tipo de activo.

COBIT 5	N/A
ITIL	N/A

2.3.4.8 OSP-8 Seguridad en el ciclo de vida de desarrollo de Software

Son necesarios procesos estructurados y controles para chequear que cada servicio instalado y sistema de información implementado cumplan con los estándares de seguridad, sean estos desarrollos internos o adquiridos externamente.

Proceso	**OSP-8- Seguridad en el ciclo de vida de desarrollo de software**
Descripción	Las organizaciones pueden elegir entre desarrollar software internamente o adquirirlo externamente. Son necesarios procesos estructurados y controles para chequear que cada servicio instalado y sistema de información cumplan con los estándares de seguridad.
Valor	Reducir los costos de mantenimiento y riesgos al negocio, tomando en cuenta el Control del Ciclo de Vida de Desarrollo de Software, desde el diseño de los sistemas de información.
Documentación	• Controles de seguridad para el desarrollo de software • Procedimiento de revisión de código
Entrada	OSP-3 Metas de seguridad de la información OSP-19 Reporte de revisión de código OSP-22 Reporte de alertas
Salida	• Análisis de seguridad del software. • Requisitos de seguridad para la adquisición de software.
Descripción de Métricas	• % de desperfectos detectados en las pruebas que impactan negativamente en la seguridad del software. • % de requerimientos de seguridad en la información que se pueden mapear en el

	diseño (puntos de control de la seguridad implementados). • Número de vulnerabilidades descubiertas que tienen mitigación. • Número de desviaciones entre el diseño y requerimientos. • Cantidad de softwares con debilidades sobre el total de softwares.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerencia de desarrollo, Gerencia de Seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-4 Gestión de cambios OSP-22 Monitoreo de alertas
Metodología o herramientas utilizadas	OWASP[8]: Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.3. Políticas y procedimientos para la operación de los sistemas informáticos y manejadores de datos. 8.2. Integridad y validez de la información. 8.4. Sistemas de información que generan el régimen informativo a remitir y/o a disposición del Banco Central de la República Argentina.
ISO 27002	12.1.1 Análisis y especificación de los requisitos de seguridad. 12.2.1 Validación de los datos de entrada. 12.2.2 Control del proceso interno. 12.2.3 Autenticación de mensajes. 12.2.4 Validación de los datos de salida. 12.3.1 Política de uso de los controles criptográficos. 12.3.2 Cifrado. 12.4.1 Control del software en explotación. 12.4.2 Protección de los datos de prueba del sistema. 12.4.3 Control de acceso a la librería de programas fuente. 12.5.3 Restricciones en los cambios a los paquetes de software.

[8] www.owasp.org

	12.5.4 Canales encubiertos y código Troyano. 12.5.5 Desarrollo externalizado del software. 12.6.1 Control de las vulnerabilidades técnicas.
COBIT 5	N/A
ITIL	N/A

2.3.4.9 OSP-9 Medidas de Seguridad de control de Cambios

Este proceso impide incidentes relacionados con los cambios de estado de las medidas de seguridad dentro de un dominio de TI.

Proceso	**OSP-9- Medidas de Seguridad de control de cambios**
Descripción	Este proceso impide incidentes relacionados con los cambios de estado de las medidas de seguridad dentro de un dominio de TI.
Valor	Los cambios en el personal de seguridad, los nuevos dispositivos de red y cambios en las medidas de seguridad representan amenazas que deben ser gestionadas.
Documentación	Procedimientos sobre medidas de seguridad para el control de cambios
Entrada	Metas de seguridad de la información TSP-3 Reporte de alertas OSP-22
Salida	Cumplimiento de medidas de seguridad por dominio de TI Reporte de control de cambio de las medidas de seguridad
Descripción de Métricas	Cantidad de cambios sobre las medidas de seguridad implementados durante un periodo de tiempo establecido
Responsabilidades	Supervisor : TSP-14 Dueño del servicio Dueño del proceso: Gerente de Seguridad de la información
Procesos Relacionados	TSP-6 Arquitectura de Seguridad OSP-5 Actualizaciones de seguridad OSP-6 Depuración/ Destrucción de activos OSP-7 Securitización de activos OSP-22 Monitoreo de alertas

Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.8. Control de cambios a los sistemas productivos.
ISO 27002	10.1 Procedimientos y responsabilidades operacionales. 10.1.2 Gestión de cambios. 12.5.1 Procedimientos de control de cambios. 12.5.2 Revisión técnica de los cambios en el sistema operativo.
COBIT 5	Dominio BAI Construir , Adquirir e implementar BAI06 Gestionar los cambios
ITIL	Fase Transición del servicio Proceso Gestión de cambios

2.3.4.10 OSP-10 Gestión de Backup

Este proceso reduce el impacto de la pérdida de información, el logro de los requisitos de nivel de servicio para el tiempo de recuperación de sistemas de información, fecha y hora del punto de recuperación y tiempo de recuperación.

Proceso	**OSP-10- Gestión de Backup**
Descripción	Este proceso reduce el impacto de perdida de información
Valor	Los incidentes derivados de la pérdida de repositorios de información, pueden ser mitigados por los procesos de copia de seguridad.
Documentación	Plan de pruebas de backup y restauración Reporte de backup Reporte de restauración Clasificación de la información
Entrada	Inventario de activos OSP-3 Reporte de detección de incidentes OSP-23 Reporte test de backup OSP-20
Salida	Reporte de backup OSP-15

	Reporte de restauración OSP-15 Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de backups exitosos sobre el total Cantidad de pruebas de restauración exitosas sobre el total
Responsabilidades	Supervisor : TSP-14 Dueño del servicio Dueño del proceso: Gerente de Seguridad de la información, Gerencia de TI
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos OSP-20 Monitoreo de alertas
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	4.1 Responsabilidades sobre la planificación de la continuidad del procesamiento de datos. 5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.
ISO 27002	10.5.1 Respaldo de la información
COBIT 5	N/A
ITIL	N/A

2.3.4.11 OSP-11 Control de Acceso

Es el proceso por el cual se provee el acceso a información clasificada a los usuarios autorizados, mientras que se deniega a los no autorizados.

Proceso	**OSP-11- Control de Acceso**
Descripción	Es el proceso por el cual se provee el acceso a información clasificada a los usuarios autorizados, mientras que se deniega a los no autorizados.
Valor	Incidentes como espionaje, denegación de responsabilidad, cambios no autorizados, pueden ser prevenidos por los procedimientos de control de acceso.
Documentación	Política de control de acceso

Entrada	• Solicitud de acceso por parte de recursos humanos • Solicitud de acceso por parte de otras áreas • Inventario de activos OSP-3
Salida	• Aprobación de acceso a usuarios autorizados • Denegación de acceso a usuarios no autorizados • Reporte de accesos no autorizados
Descripción de Métricas	• % de intentos fallidos de acceso a activos críticos. • % de accesos de emergencia en que se cumplió con el procedimiento. • Ranking de usuarios de emergencias más utilizados.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos OSP-12 Registro de usuarios
Metodología o herramientas utilizadas	Herramientas de gestión de peticiones
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.2. Estrategia de seguridad de acceso a los activos de información. 3.1.4. Política de protección. 3.1.4.1. Clasificación de los activos de información - Niveles de acceso a los datos. 3.1.4.2. Estándares de acceso, de identificación y autenticación, y reglas de seguridad. 3.1.5.1. Control y monitoreo. 5.8. Control de cambios a los sistemas productivos. 6.4. Operatoria y control de las transacciones cursadas por medio de Internet (e-banking).
ISO 27002	11.2.1 Registro de usuarios. 11.2.2 Gestión de privilegios.
COBIT 5	Catalizador Información - Dimensiones Metas de Accesibilidad y Disponibilidad Acceso restringido
ITIL	Fase Operación del servicio Proceso Gestión de acceso a los servicios TI

2.3.4.12 OSP-12 Registro de Usuarios

Este proceso cubre la inscripción que permite vincular cuentas de usuario certificados con sus dueños identificables o anónimos y gestiona el ciclo de vida de cuentas de usuario y certificados.

Proceso	OSP-12- Registración de usuarios
Descripción	Este proceso cubre la inscripción que permite vincular cuentas de usuario certificados con sus dueños identificables o anónimos y gestiona el ciclo de vida de cuentas de usuario y certificados.
Valor	• Hacer que los usuarios sean responsables por el uso que le dan a los servicios, interfaces y repositorios. • Prevención y mitigación de los incidentes surgidos de la concesión inapropiada de acceso, a través de procedimientos de registración de usuarios.
Documentación	• Política de control de acceso • Procedimiento de requerimiento de acceso
Entrada	Inventario de activos OSP-3 Requerimiento de acceso (De usuarios) Lista de egresos – RRHH Cambios de estado del personal TSP-8
Salida	Registro de usuario Identificador único de usuario Registración denegada Modificación de usuarios Baja de cuentas
Descripción de Métricas	• % de sistemas de control de acceso para los cuales la contraseña para el primer login no es previsible. • % de sistemas de control de acceso que requieren el cambio de contraseña al primer login. • % de sistemas de control de acceso para los cuales expiran las cuentas de usuario no utilizadas.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos

	OSP-14 Protección de ambientes físicos OSP-16 Gestión de tráfico de redes
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.4. Política de protección.
ISO 27002	11.2.1 Registro de usuarios.
COBIT 5	N/A
ITIL	N/A

2.3.4.13 OSP-14 Protección de ambientes físicos

Este proceso cubre el control de acceso a áreas seguras que contienen repositorios o interfaces importantes, así como a instalaciones alternativas.

Proceso	**OSP-14- Protección de ambientes físicos**
Descripción	Este proceso cubre el control de acceso a áreas Seguras que contienen repositorios o interfaces importantes, así como a instalaciones alternativas.
Valor	Prevención y mitigación de los incidentes causados por la explotación directa de los activos y por el daño físico a los mismos, mediante medidas eficaces de seguridad física.
Documentación	Procedimiento de control de acceso físico Procedimiento de control ambiental
Entrada	Inventario de activos OSP-3
Salida	• TSP 4 - Registros de acceso físico • TSP4 - Registro de condiciones ambientales
Descripción de Métricas	• % de los incidentes de seguridad física donde se permitió la entrada a personal no autorizado a las instalaciones que contienen sistemas de información. • % de los incidentes de pérdida de disponibilidad ocasionados por factores ambientales.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso

	Dueño del Proceso : Gerente de instalaciones
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos OSP-12 Registración de usuarios OSP-15 Gestión de continuidad de operaciones OSP-23 Detección y análisis de eventos internos
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.2. Implementación de los controles de seguridad física aplicados a los activos de información.
ISO 27002	9.1.1 Perímetro de seguridad física. 9.1.2 Controles de acceso físico. 9.1.4 Protección contra amenazas externas y ambientales. 9.1.5 Trabajo en áreas seguras. 9.1.6 Áreas de carga, despacho y acceso público.
COBIT 5	N/A
ITIL	N/A

2.3.4.14 OSP-15 Gestión de continuidad de operaciones

Este proceso utiliza redundancia y dispersión para eliminar puntos críticos de falla y reducir el impacto de incidentes que puedan amenazar la existencia de la organización; alcanzando requerimientos regulatorios y del negocio para recuperación de los procesos del mismo en un tiempo acotado, como así también fecha y hora de puntos de revisión.

Proceso	**OSP-15- Gestión de Continuidad de operaciones**
Descripción	Este proceso utiliza redundancia y dispersión para eliminar puntos críticos de falla y reducir el impacto de incidentes que puedan amenazar la existencia de la organización; alcanzando requerimientos regulatorios y del negocio para

	recuperación de los procesos del mismo en un tiempo acotado, como así también fecha y hora de puntos de revisión.
Valor	La gestión de la continuidad de las operaciones podría evitar que la organización se vea seriamente afectada ante la existencia de eventos que puedan causar dificultad sobre la prestación constante de los servicios, ocasionando la posible pérdida de clientes.
Documentación	Política de gestión de disponibilidad Procedimiento de continuidad de operaciones Plan de evaluación de continuidad de operaciones
Entrada	Inventario de Activos (OSP-3). Reporte de backup OSP-10 Reporte de restore OSP-10 Reporte de detección de incidentes (OSP-23). Análisis de impacto en el negocio (BIA).
Salida	Protección de la existencia de la organización Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de pruebas realizadas al plan de continuidad de operaciones durante un periodo establecido
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Inventario de activos OSP-20 Emulación de incidentes OSP-23 Detección y análisis de eventos internos
Metodología o herramientas utilizadas	BS 25999 ISO 22301
Mapeo a otros Frameworks o Normativa	
Normativa 4609	4.1. Responsabilidades sobre la planificación de la continuidad del procesamiento de datos. 4.2. Análisis de impacto. 4.3. Instalaciones alternativas de procesamiento de datos. 4.4. Plan de continuidad del procesamiento de datos. 4.5. Mantenimiento y actualización del plan de continuidad de procesamiento de datos. 4.6. Pruebas de continuidad del procesamiento de datos.

	5.2. Inventario tecnológico. 5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base. 5.10. Manejo de incidentes. 7.7. Planificación de continuidad de la operatoria delegada.
ISO 27002	14.1.1 Incluir la seguridad de la información en el proceso de gestión de la continuidad del negocio. 14.1.2 Continuidad del negocio y evaluación de riesgos. 14.1.3 Desarrollar e implementar planes de continuidad incluyendo la seguridad de la información. 14.1.4 Marco de trabajo del planeamiento de la continuidad del negocio. 14.1.5 Prueba, mantenimiento y reevaluación de planes de continuidad del negocio.
COBIT 5	Dominio entregar, Dar servicio y soporte DSS04 Gestionar la continuidad
ITIL	Fase Diseño del servicio Proceso Gestión de la continuidad de los servicio TI

2.3.4.15 OSP-16 Gestión de Trafico de Redes

Este proceso define políticas técnicas para la gestión del tráfico de mensajes/paquetes de datos autorizados entre zonas, detectando y denegando el tráfico no autorizado, definiendo políticas de cifrado.

Proceso	**OSP-16- Gestión de tráfico de redes**
Descripción	Este proceso define políticas técnicas para la gestión del tráfico de mensajes/paquetes de datos autorizados entre zonas, detectando y denegando el tráfico no autorizado, definiendo políticas de cifrado.
Valor	La segmentación apropiada de dominios de TI y repositorios, junto con el filtrado de mensajes/paquetes, pueden prevenir y mitigar

	incidentes causados por intrusión, vandalismo y mal uso de sistemas de información.
Documentación	Procedimientos de definición de DMZ[9] Reporte de filtrado de autorizaciones Procedimiento de detección de intrusión
Entrada	Topología de red Inventario de activos OSP-3 Reporte de detección de intrusiones OSP-23
Salida	Reportes de reglas de filtrado (TSP-4). Logs de bloqueos (OSP-23). Logs de autorizados (OSP-23). Reporte de Métricas (TSP-4).
Descripción de Métricas	• Número de reglas de firewall configuradas por mes. • Cantidad de reglas de firewall por cantidad de bloqueos. • Cantidad de firmas por cantidad de bloqueos. • Cantidad de Spam por cantidad de bloqueos.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos OSP-12 Registración de usuarios OSP-23 Detección y análisis de eventos internos
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.4. Política de protección. 6.4. Operatoria y control de las transacciones cursadas por medio de Internet (e-banking).
ISO 27002	10.6.1 Controles de red. 10.6.2 Seguridad en los servicios de redes.
COBIT 5	N/A
ITIL	N/A

[9] zona desmilitarizada – Donde los Servidores públicos se colocan en un segmento diferente de red

2.3.4.16 OSP-17 Gestión de protección contra código malicioso

Conjunto de medidas de seguridad para proveer protección contra amenazas técnicas como virus, spyware, troyanos, backdoors, key loggers, rootkits, y otros servicios no autorizados.

Proceso	**OSP-17- Gestión de protección contra código malicioso**
Descripción	Conjunto de medidas de seguridad para proveer protección contra amenazas técnicas como virus, spyware, troyanos, backdoors, key loggers, rootkits, y otros servicios no autorizados.
Valor	Un proceso adecuado de protección contra código malicioso permite prevenir y/o mitigar el nivel de incidentes relacionados con la infección de activos informáticos.
Documentación	Procedimiento de protección contras software malicioso Reporte de detección y eliminación de software malicioso
Entrada	Gestión de activos OSP-3 Detección y análisis de eventos internos OSP-23
Salida	• Protección de sistemas de información • Reporte de detección y eliminación de código malicioso (OSP-23). • Reporte del nivel de actualización y protección ante la propagación de código malicioso (TSP-4). • Reporte de métricas (TSP-4).
Descripción de Métricas	• Nivel de actualización contra código malicioso para cada sistema de información. Es igual al número de días de antigüedad de las actualizaciones conocidas pero no aplicadas. • Número de equipos desactualizados.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-2 Adquisición en seguridad OSP-3 Gestión de activos OSP-23 Detección y análisis de eventos externos

Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.4.5. Alertas de seguridad y software de análisis. 3.1.4.6. Software malicioso.
ISO 27002	10.4.1 Controles contra código malicioso.
COBIT 5	N/A
ITIL	N/A

2.3.4.17 OSP-19 Auditoría Técnica Interna

Este proceso permite validar lo siguiente:

- Eficacia de las medidas de reducción de vulnerabilidad
- Eficacia de las medidas de control de acceso
- Eficacia de las medidas de registro de usuario
- Eficacia de las medidas de filtrado
- Calidad del software de desarrollo propio

Proceso	**OSP-19- Auditoria técnica interna**
Descripción	Este proceso permite validar lo siguiente: • Eficacia de las medidas de reducción de vulnerabilidad • Eficacia de las medidas de control de acceso • Eficacia de las medidas de registro de usuario • Eficacia de las medidas de filtrado • Calidad del software de desarrollo propio
Valor	Los incidentes derivados de la explotación de las vulnerabilidades en la configuración del software y en torno a las fronteras de la organización se pueden prevenir mediante emulación de ataques, reparación de software, securitización de activos, inversión y un mejor control.

Documentación	Política de auditoria Procedimiento de emulación de ataques Procedimiento de revisión de código fuente Procedimiento de control de acceso y registración de usuarios Procedimiento de reglas de filtrado
Entrada	Inventario de activos
Salida	Reporte de emulación de ataques OSP-4 Reporte de revisión de código fuente OSP-8 Reporte de revisión de accesos y registración de usuarios OSP-11 OSP-12 Informe de reglas de filtrado TSP-4 Reporte de métricas TSP-4
Descripción de Métricas	• % de debilidades que son falsos negativos • % de debilidades no encontradas
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información o Auditor independiente
Procesos Relacionados	OSP-4 Seguridad en la gestión de cambios OSP-8 Seguridad en el ciclo de vida de desarrollo de Software OSP-9 Medidas de seguridad de control de cambios OSP-11 Control de Acceso OSP-12 Registración de usuarios OSP-14 Protección en ambientes físicos OSP-16 Gestión de tráfico de redes OSP-17 Gestión de protección contra código malicioso
Metodología o herramientas utilizadas	OWASP[10]
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.4.4. Registros de seguridad y pistas de auditoría.
ISO 27002	15.2.1 Cumplimiento de políticas y estándares de seguridad. 15.2.2 Verificación de cumplimiento técnico. 15.3.1 Controles de auditoría de sistemas de información.

[10] Open Web Application Security Project – proyecto para combatir el diseño de software inseguro

	15.3.2 Protección de herramientas de auditoría de sistemas de información
COBIT 5	Dominio Supervisar, evaluar y valorar MEA01 Supervisar, evaluar y valorar rendimiento y conformidad
ITIL	N/A

2.3.4.18 OSP-20 Emulación de Incidentes

Este proceso valida la efectividad de los procesos OSP-10: Gestión de copia de seguridad, OSP-26: Gestión de infraestructura critica de seguridad, OSP-15: Gestión de la Continuidad de Operaciones, procesos encargados de proteger accidentes, errores y el fracaso de las medidas de reducción de vulnerabilidades. Este proceso puede llevarse a cabo mediante pruebas de todos los posibles objetivos o una muestra aleatoria representativa de ellos.

Proceso	**OSP-20- Emulación de incidentes**
Descripción	Este proceso valida la efectividad de los procesos OSP-10: Gestión de backup, OSP-26: Gestión de infraestructura critica de seguridad, OSP-15: Gestión de la Continuidad de Operaciones, procesos encargados de proteger accidentes, errores y el fracaso de las medidas de reducción de vulnerabilidades.
Valor	El impacto de los principales incidentes se puede mitigar mediante la emulación del mismo, en el que la prueba prevista se utiliza para simular un incidente con el fin de mejorar la respuesta a la emergencia y las medidas de reducción de impacto.
Documentación	Plan de pruebas de copias de seguridad y restore Plan de pruebas de continuidad de operaciones Pruebas de emulación de incidentes Política de auditoria
Entrada	TSP-3 Objetivos y metas de seguridad
Salida	Reporte pruebas de copias de seguridad y restore OSP-10 OSP-15

	Reporte de pruebas de continuidad de operaciones OSP-15 , GP-3 Reporte de métricas TSP-4
Descripción de Métricas	Cantidad de restauraciones exitosas % cumplimiento plan de continuidad
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de TI), (Tester), Gerente de Seguridad de la información (Tester) o auditor independiente
Procesos Relacionados	OSP-10 Gestión de backup OSP-15 Gestión de continuidad de operaciones OSP-26 Gestión de infraestructura critica de seguridad TSP-13 Gestión de seguros
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	Ver mapeo a procesos OSP-10, OSP-15, OSP-26
ISO 27002	
COBIT 5	
ITIL	

2.3.4.19 OSP-21 Calidad de Información y evaluación de Cumplimiento

Revisión periódica de la información clasificada en poder de dar la garantía de que está completa, exacta, actualizada, y se mantuvo durante un fin determinado de acuerdo con la ley y la ética de la empresa y los contratos.

Proceso	**OSP-21- Calidad de información y evaluación de cumplimiento**
Descripción	Revisión periódica de la información clasificada con el fin de garantizar que es completa, exacta, actualizada, y se mantuvo durante un fin determinado de acuerdo con la ley y la ética de la empresa y los contratos establecidos.
Valor	Los incidentes ocasionados por una mala clasificación de la información, a nivel de

	completitud, exactitud y expiración pueden ser mitigados con un proceso de calidad
Documentación	Plan de auditoria Requerimientos normativos
Entrada	Inventario de activos OSP-3 Requerimientos normativos Issues de cumplimiento
Salida	Identificación de riesgos de cumplimiento Estado de cumplimiento Métricas de cumplimiento
Descripción de Métricas	Cantidad de issues remediados por periodo de auditoria Estado de cumplimiento por ente de control (interno – Externo)
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad informática o auditor independiente
Procesos Relacionados	Todos los procesos del modelo
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	Todas las secciones de la normativa
ISO 27002	15.1 Conformidad con los requisitos legales
COBIT 5	Dominio Supervisar, evaluar y valorar MEA-03 Supervisar, Evaluar y Valorar la Conformidad con los requerimientos externos
ITIL	N/A

2.3.4.20 OSP-22 Monitoreo de Alertas

Este proceso valida que se realice un monitoreo sobre los umbrales de capacidad y rendimiento de los activos de información de la organización.

Proceso	OSP-22- Monitoreo de Alertas
Descripción	Este proceso valida que se realice un monitoreo sobre los umbrales de capacidad y rendimiento de los activos de información de la organización
Valor	Incidentes causados por la explotación de las debilidades publicados en los productos de software se pueden prevenir mediante la aplicación oportuna de las medidas correctivas. La debilidad de los sistemas de producción descubierto por empleados o terceros requiere una acción correctiva. Las nuevas amenazas pueden requerir cambios en el SGSI.
Documentación	Procedimiento de monitoreo de alertas Monitoreo de la política de seguridad
Entrada	Informes de debilidades, correcciones y amenazas (internos y externos) Gestión de activos OSP-3
Salida	Informe de alertas, amenazas y correcciones realizadas Reporte de métricas TSP-4
Descripción de Métricas	% de alertas detectados como falsos positivos % de alertas detectados como falsos negativos
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de Seguridad de la información
Procesos Relacionados	OSP-4 Seguridad en la gestión de cambios OSP 4 - Seguridad en el Control de Cambios. OSP 8 - Seguridad en el Ciclo de Vida de Desarrollo de Software. OSP-9 Medidas de seguridad de control de cambios OSP 16 - Gestión de Tráfico de Redes. OSP 17 - Gestión de Protección contra Código Malicioso.
Metodología o herramientas utilizadas	Herramientas utilizadas para monitoreo de alertas
Mapeo a otros Frameworks o Normativa	
Normativa 4609	3.1.5.1 Control y monitoreo
ISO 27002	10.10.2 Monitoreo del uso del sistema. 10.10.3 Protección de la información del registro. 10.10.4 Registros del administrador y del operador.

	10.10.5 Registro de fallas. 10.10.6 Sincronización de relojes. 12.6.1 Control de vulnerabilidades técnicas
COBIT 5	Dominio Construir, Adquirir e implementar BAI04 Gestionar la Disponibilidad y la Capacidad
ITIL	Fase Diseño del servicio Proceso Gestión de la capacidad Proceso Gestión de la disponibilidad

2.3.4.21 OSP-23 Detección y Análisis de eventos internos

Este proceso mediante el análisis de logs generados por los sistemas permite detectar y analizar posibles eventos que atenten contra la seguridad de la información.

Proceso	**OSP-23- Detección y análisis de eventos internos**
Descripción	Este proceso mediante el análisis de logs generados por los sistemas permite detectar y analizar posibles eventos que atenten contra la seguridad de la información.
Valor	• Gestionar el riesgo de manera efectiva, por medio de una detección temprana de eventos que pueda evitar compromiso a la seguridad. • Detectar incidentes puede evitar que se repitan o den lugar a incidentes con un mayor impacto; lo que resultaría en daños crónicos a los sistemas de información y el incumplimiento de los objetivos de seguridad. • Reducir a un nivel aceptable los riesgos internos y externos de concreción de incidentes.
Documentación	Procedimiento de detección de intrusión e incidentes Reporte de detección de incidentes Reporte de detección de intrusión
Entrada	Eventos Logs de bloqueos OSP-16 Logs de autorizados OSP-16

	Reporte de detección y eliminación de software malicioso OSP-17 Inventario de activos OSP-3
Salida	Incidentes e intrusiones detectadas Reporte de detección de incidentes OSP-10-OSP-15, OSP-16, OSP-17, OSP-24, OSP-26 Reporte de detección de intrusiones OSP-16, OSP-24 Reporte de métricas TSP-4
Descripción de Métricas	• % de aplicaciones que son monitoreadas (sobre el total de aplicaciones). • % de BD que son monitoreadas (sobre el total de BD). • % de servicios de IT que son monitoreados (por ej., Chat, Correo, acceso a Internet). • % de activos que son monitoreados (sobre el total de activos).
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de Seguridad de la información
Procesos Relacionados	OSP-10 - Gestión de copias de seguridad OSP 16 - Gestión de Tráfico de Redes. OSP 17 - Gestión de Protección contra Código Malicioso. OSP-26 - Gestión de infraestructura critica de seguridad
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.10 Manejo de incidentes
ISO 27002	13. Gestión de incidentes de seguridad
COBIT 5	Dominio Entregar, dar servicio y soporte DSS02 Gestionar las peticiones y los incidentes del servicio
ITIL	Fase Operación del servicio Proceso Gestión de eventos

2.3.4.22 OSP-24 Gestión de incidentes

Este proceso apunta a limitar el impacto de incidentes y vulnerabilidades de seguridad mediante un seguimiento efectivo.

Proceso	OSP-24- Gestión de incidentes
Descripción	Este proceso apunta a limitar el impacto de incidentes y vulnerabilidades de seguridad mediante un seguimiento efectivo.
Valor	• Procedimientos claros y precisos para el manejo de incidentes de seguridad pueden ayudar a mitigar los efectos de un incidente y prevenir futura recurrencia. • La información de incidentes puede ser usada para medir la eficiencia de las medidas de seguridad, mejorar las mismas, y tomar decisiones sobre inversión en seguridad. Los incidentes impactan en la gestión de riesgo tecnológico, teniendo como efecto el refuerzo de ciertos controles que se efectúan a cada uno de los activos.
Documentación	Procedimiento de respuesta ante incidentes Reporte de incidentes Reporte de intrusión
Entrada	Reporte de incidentes OSP-23 Reporte de intrusión OSP-23
Salida	Reporte de incidentes OSP-25, TSP-10 Reporte de Intrusión OSP-25 Reporte de métricas TSP-4
Descripción de Métricas	• % de incidentes de seguridad reportados dentro de un margen de tiempo establecido por categoría/canal. • % de incidentes de seguridad solucionados dentro de un margen de tiempo establecido por categoría/canal, reportados dentro del margen de tiempo establecido por categoría/canal. • % de incidentes de seguridad críticos. • % de incidentes de seguridad sobre activos críticos.

	• Cantidad de oportunidades de mejora propuestas. • Análisis de tendencias de incidentes de seguridad por categoría/canal.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso Dueño del proceso: Gerente de seguridad de la información
Procesos Relacionados	OSP-23 Detección y análisis de eventos internos OSP-25 Informática forense
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.10 Manejo de incidentes
ISO 27002	13. Gestión de incidentes de seguridad
COBIT 5	Dominio Entregar, dar servicio y soporte DSS02 Gestionar las peticiones y los incidentes del servicio
ITIL	Fase Operación del servicio Proceso Gestión de eventos

2.3.4.23 OSP-25 Informática forense

Este proceso investiga y diagnostica la secuencia, la autoría, la clasificación, la causa subyacente, y el impacto de los incidentes.

Proceso	**OSP-25- Informática forense**
Descripción	Este proceso investiga y diagnostica la secuencia, la autoría, la clasificación, la causa subyacente, y el impacto de los incidentes.
Valor	La informática forense se puede utilizar para: Evaluar un incidente Identificar las medidas correctivas Como apoyo para la persecución de los atacantes, si es el caso.
Documentación	Procedimiento de evaluación de informática forense
Entrada	Reporte de incidentes OSP-24

	Reporte de intrusión OSP-24
Salida	Investigación de incidentes e intrusiones Reporte de informática forense TSP-4, TSP-10 y procedimientos legales Reporte de métricas TSP-4
Descripción de Métricas	% de informes de informática forense que sean falsos positivos o falsos negativos
Responsabilidades	Supervisor: TSP-14 Dueño del servicio Dueño proceso: Gerente de seguridad informática
Procesos Relacionados	OSP-24 Gestión de incidentes
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	N/A
ISO 27002	13.2.3 Recolección de evidencia
COBIT 5	N/A
ITIL	N/A

2.3.4.24 OSP-26 Gestión de infraestructura critica de seguridad

Este es un conjunto de medidas de seguridad basadas en redundancia, diversidad y dispersión, para eliminar puntos de falla y reducir el impacto de pérdida y falla de la infraestructura crítica de seguridad. El objetivo es alcanzar un nivel de servicio que permita recuperar la protección de los activos en un tiempo medio breve.

Proceso	**OSP-26- Gestión de infraestructura critica de seguridad**
Descripción	Este es un conjunto de medidas de seguridad basadas en redundancia, diversidad y dispersión, para eliminar puntos de falla y reducir el impacto de pérdida y falla de la infraestructura crítica de seguridad.
Valor	Incidentes como la pérdida de logs de seguridad

	y la disrupción de interfaces y servicios de seguridad pueden ser mitigados a través de la eliminación de puntos de falla y la incorporación de resilencia para fallas parciales o totales.
Documentación	Plan de pruebas de capacidad y disponibilidad Política de gestión de disponibilidad
Entrada	Inventario de activos OSP-3 Reporte de detección de incidentes OSP-23
Salida	• Prevención de pérdida permanente de logs de información • Prevención de disrupción de interfaces y servicios de seguridad.
Descripción de Métricas	• % de tiempo de disponibilidad, por servicio por periodo de tiempo establecido • Cantidad de incidentes de falla de infraestructura crítica; por servicio por periodo de tiempo establecido • Cantidad de incidentes de falla de infraestructura crítica; según exista o no contrato de mantenimiento y soporte sobre el servicio. afectado, por periodo de tiempo establecido. • Promedio de tiempos de recuperación ante fallas de infraestructura crítica, por periodo de tiempo establecido
Responsabilidades	Supervisor: TSP-14 Dueño de proceso Dueño de Proceso: Gerente de TI, Gerente de Seguridad de la información
Procesos Relacionados	OSP-2 OSP-3 Inventario de activos OSP-20 Emulación de incidentes OSP-23 Detección y análisis de eventos internos
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	9.2.4 Mantenimiento del equipamiento. 10.5.1 Copia de respaldo de la información.
ISO 27002	2.3. Análisis de Riesgos. 4.2. Análisis de impacto.
COBIT 5	Dominio Entregar, Dar Servicio y soporte DSS05 Gestionar los servicios de seguridad
ITIL	N/A

2.3.4.25 OSP-27 Gestión de archivo

Se trata de un conjunto de medidas de seguridad para garantizar que el acceso a la información, se encuentra almacenada de acuerdo a los requisitos establecidos para períodos de retención.

Proceso	**OSP-27- Gestión de archivo**
Descripción	Se trata de un conjunto de medidas de seguridad para garantizar la accesibilidad de la información que se encuentra almacenada de acuerdo a los requisitos establecidos para largos períodos de retención.
Valor	La información a recuperar debe estar correctamente almacenada, catalogada y monitoreada de forma periódica, con el fin de evitar incidentes derivados de la perdida de repositorios de información implementados para largos periodos de retención
Documentación	Pruebas al plan de restauración de archivo Reporte de restauración de archivo Política de gestión de disponibilidad
Entrada	Inventario de activos OSP-3
Salida	Prevención de perdida de información almacenada en los repositorios definidos para tal fin Reporte de almacenamiento de archivo Reporte de restauración de archivo
Descripción de Métricas	% de repositorio próximos a la terminación de su vida útil
Responsabilidades	Supervisor: TSP-14 Dueño de proceso Dueño de Proceso: Gerente de TI, Gerente de Seguridad de la información
Procesos Relacionados	OSP-3 Inventario de activos OSP-6 Depuración y/o destrucción de activos de información
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de

	base. 9.2.4 Mantenimiento del equipamiento
ISO 27002	9.2.4 Mantenimiento de los equipos
COBIT 5	Dominio Construir, Adquirir e implementar BAI04 Gestionar la Disponibilidad y la Capacidad
ITIL	Fase Diseño del servicio Proceso Gestión de la capacidad Proceso Gestión de la disponibilidad

2.3.4.26 OSP-28 Detección y Análisis de eventos externos

Este proceso puede tomar medidas de carácter técnico o legal a través de :

- Las opiniones y los ataques contra la reputación de la organización en línea
- Phishing y la tergiversación de la organización
- Violación de derechos de autor

Proceso	**OSP-28- Detección y análisis de eventos externos**
Descripción	Este proceso puede tomar medidas de carácter técnico o legal a través de : • Las opiniones y los ataques contra la reputación de la organización en línea • Phishing y la tergiversación de la organización • Violación de derechos de autor
Valor	Los daños a la reputación, el phishing, la tergiversación de la organización, y la violación de los derechos de autor deben ser prevenidos y mitigados.
Documentación	Procedimiento de detección de incidentes externos Politica de manejo de incidentes Reporte de phising, violación de derecho de autor
Entrada	Reporte de violación de copyright Inventario de activos OSP-3
Salida	Reporte de detección de incidentes OSP-10,

	OSP-15, OSP-16, OSP-17, OSP-24, OSP-26 Reporte de intrusión de incidentes OSP-16, OSP-24
Descripción de Métricas	Cantidad de intentos de phising realizados durante un periodo de tiempo establecido
Responsabilidades	Supervisor: TSP-14 Dueño de proceso Dueño de Proceso: Gerente de seguridad de información.
Procesos Relacionados	OSP-10 Gestión de backup OSP-16 Gestión de tráfico de red OSP-17 Gestión de protección contra código malicioso OSP-24 Detección y análisis de eventos internos OSP-26 Gestión de infraestructura critica de seguridad
Metodología o herramientas utilizadas	N/A
Mapeo a otros Frameworks o Normativa	
Normativa 4609	
ISO 27002	15.1.2 Derechos de propiedad intelectual
COBIT 5	N/A
ITIL	N/A

3. Especificación de Métricas

Las métricas permiten a las áreas de seguridad de la información formular indicadores de desempeño sobre los productos, procesos o servicios que ofrecen, facilitando la toma de decisiones, ya que de ellas se obtiene la recopilación y análisis de datos importantes. Dichas decisiones sirven como soporte para la asignación de recursos, capacitaciones, mejoras de procesos, etc. Existen diferentes estándares que proponen métricas de seguridad, algunos de ellos son: NIST[11] 800-55, ISO27004, CISWG[12], entre otros.

3.1 Tipos de métricas

De acuerdo al NIST 800-55, existen 3 tipos de métricas de seguridad, que permiten establecer un programa de seguridad de la información lo suficientemente maduro en relación al rendimiento de los procesos definidos para el área.

Los tres tipos de métricas que proponen las NIST son las siguientes:

- Métricas de implementación
- Métricas de eficacia y eficiencia
- Métricas de impacto en el negocio

3.1.1 Métricas de implementación

Se utilizan para demostrar el progreso en la implementación de programas de seguridad de la información, controles de seguridad específicos,

[11] NIST National Institute of Standards Technology

[12] Corporate information security working group

políticas y procedimientos asociados. Su progreso se mide a través de porcentaje o cantidad de implementación llevada a cabo.

Ejemplo: % de servidores de la organización a los que se les ha aplicado una configuración estándar.

3.1.2 Métricas de eficacia y eficiencia

Este tipo de métricas están diseñadas para monitorear si los controles de seguridad están funcionando de acuerdo a la planeación realizada y si se están obteniendo los resultados esperados. Estos controles se enfocan en las pruebas realizadas y en los resultados que espera cubrir la organización en temas asociados a la seguridad de la información.

Ejemplo: Cantidad de parche de seguridad que han cubierto las vulnerabilidades encontradas.

3.1.3 Métricas de impacto en el negocio

Son utilizadas para articular el impacto de la seguridad de la información sobre la misión de organización. Dependiendo de la misión que tenga la empresa este tipo de métricas pueden ser utilizadas para cuantificar el ahorro de costos en relación a eventos de seguridad, así como el grado de confanza que la organización proyecta hacia sus clientes y proveedores.

Ejemplo: % de asignación del presupuesto de TI asociado a la seguridad de la información

En relación a estándares como ISM3, NIST 800-55, ISO 27004 y CISWG[13], a continuación se relaciona algunas métricas para algunos procesos operacionales del modelo, de acuerdo a su tipo.

Convención utilizada

IM: Métricas de implementación

EF: Métricas de eficacia y eficiencia

NE: Métricas de impacto en el negocio

Cod_Proc	Proceso	Tipo de métrica	Ejemplo de Métrica para evaluar el proceso
OSP-1	Reporte de la Gestión Operacional de la Seguridad	EF	• Número de vulnerabilidades descubiertas.
OSP-2	Adquisición en Seguridad	IM	• Número de incidentes de seguridad causados por la selección de proveedores y productos/servicios que no cumplieron con los objetivos fijados.
		IM	• % de proveedores con los cuales se ha establecido un acuerdo de nivel de servicio.
OSP-3	Gestión de inventario de Activos de información	IM	• % de procesos de negocio en el inventario
		IM	• % de procesos de soporte en el inventario
		IM	• % de aplicaciones en el inventario
OSP-4	Seguridad en el Control de Cambios	EF	• % de cambios en los que se detectaron vulnerabilidades de seguridad.
		IM	• % de cambios no autorizados por vulnerabilidades de seguridad
OSP-5	Actualización de Seguridad	EF	• Cantidad de parches de seguridad que se implementaron para hacer frente a las vulnerabilidades identificadas.
		IM	• Número de parches de seguridad pendientes de implementación, por criticidad y tipo de tecnología.
OSP-6	Depuración y/o Destrucción de Activos de Información	IM	• % de activos dados de baja del inventario y que cuentan con confirmación formal de borrado o destrucción.
		EF	• Tiempo de respuesta promedio ante requerimientos de depuración de activos.

Tabla 2 – Ejemplos Tipo de Métricas

[13] Corporate information security working group

4 Modelo de seguridad propuesto

Como se ha mencionado en el transcurso del presente trabajo el modelo ISM3 propone procesos de seguridad de acuerdo a niveles (genéricos, estratégicos, tácticos y operativos), con el fin de lograr estructurar estos procesos se toma como base el modelo de procesos propuesto por cobit 5[14] que define una separación de los mismos a nivel de gobierno y gestión.

El alcance de procesos a nivel de gobierno de TI empresarial se define en el siguiente dominio:

- EDM: Evaluar, Orientar y Supervisar

A nivel de gestión de TI empresarial, los procesos están definidos en los siguientes dominios:

- APO: Alinear, Planificar y Organizar
- BAI: Construir, Adquirir e Implementar
- DSS: Entregar, Dar Soporte y Servicio
- MEA: Supervisar, Evaluar y Valorar

Teniendo como base lo anteriormente mencionado a continuación en la figura 4 se detalla el modelado de procesos ISM3:

[14] Marco de negocio para el gobierno y la gestión de las TI de la empresa

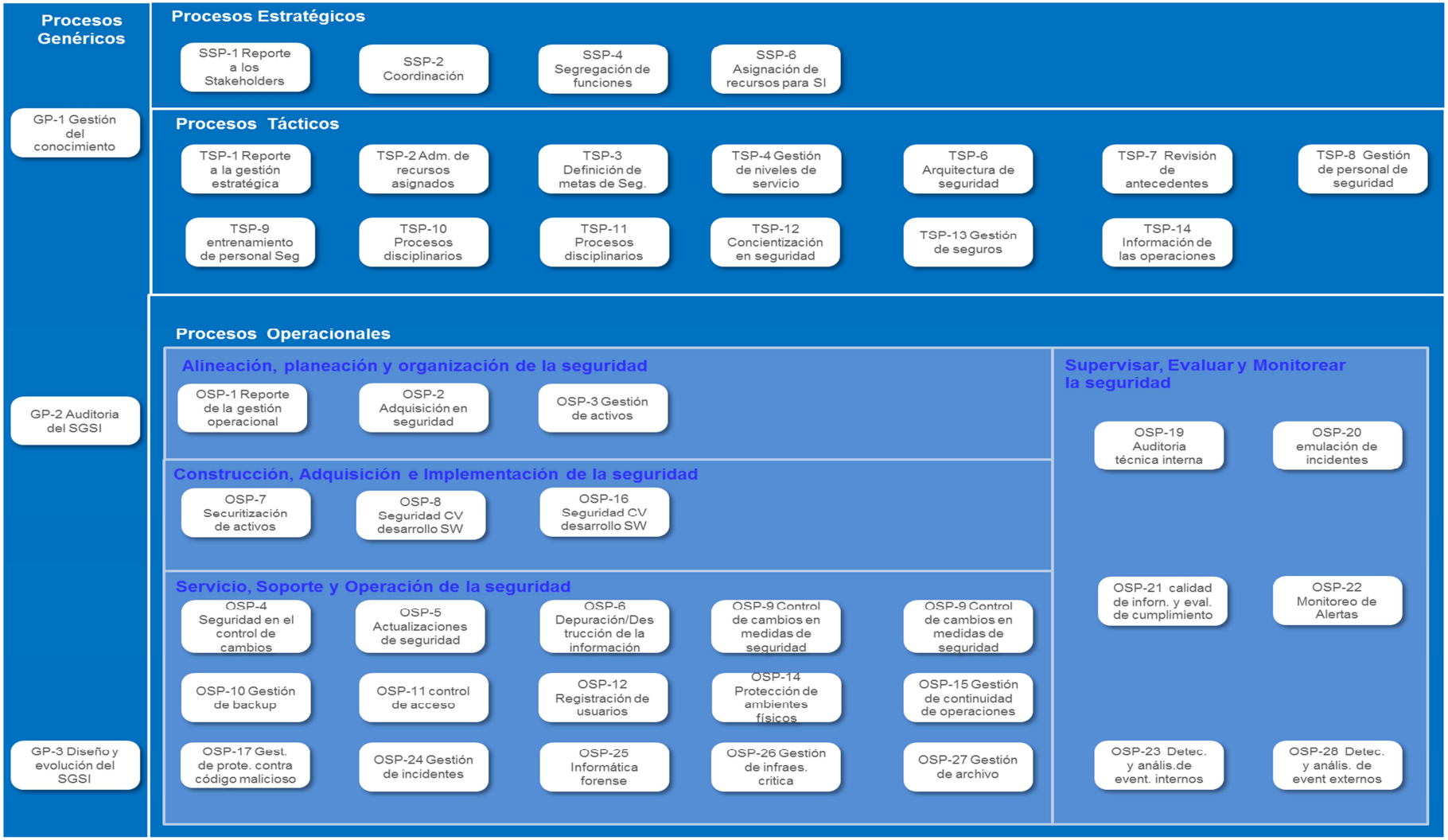


Figura 4 - Modelado de procesos ISM3. Alineación con Cobit 5 – Fuente: ISACA –Cobit 5

5 Modelo de Madurez

Un modelo de madurez permite definir un método de evaluación eficiente para los procesos de seguridad logrando de esta forma, poder establecer el nivel en que se encuentra y además tomar decisiones acordes a las necesidades de cada uno de ellos

Cobit 4.1 propone un modelo de madurez que tiene como base los siguientes fundamentos:

- Existen 5 niveles propuestos para la madurez de los procesos, los mismos de detallan en la figura 5.
- Adicionalmente establecer criterios para definir el nivel, basado en los siguientes atributos:
    - Conciencia y comunicación (CC): Entender el grado de conciencia respecto a las necesidades y prioridades del negocio, los compromisos del área, los activos críticos, y el nivel de los mecanismos de comunicación que se utilizan.
    - Políticas, estándares y procedimientos (PP): Entender el grado en el que Protección de Activos se apoya en sus procesos y sobre la calidad de estos. ¿Se revisan, se optimizan, se incorporan buenas prácticas o estándares externos?.
    - Herramientas y automatización (HA): Entender si se utilizan herramientas manuales o automáticas; y si éstas están estandarizadas, integradas, y si los procesos se apoyan en ellas.
    - Habilidades y experiencia (HE): Entender si se conocen las habilidades necesarias para el área y si se cuenta con ellas.
    - Responsabilidad y rendición de cuentas (RE): Entender los niveles de responsabilidad establecido para cada integrante del área de seguridad.
    - Establecimiento y medición de metas: (ME): Determinar si se implementaron sistemas de medición de desempeño de los procesos

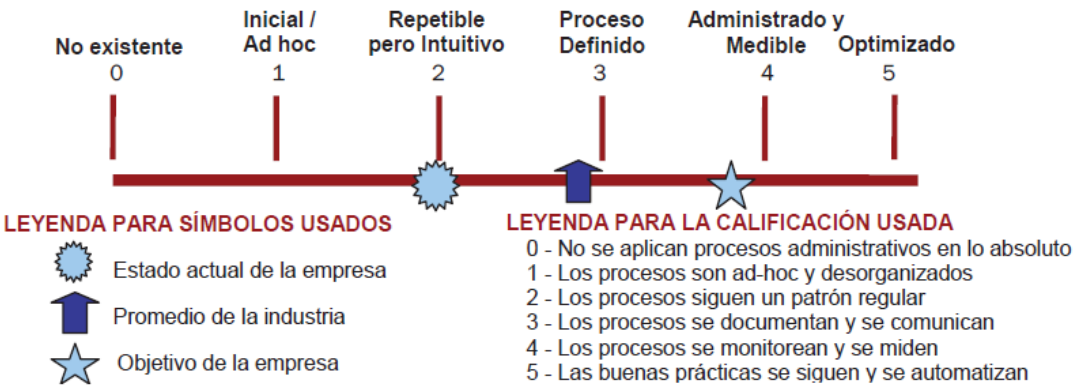


Figura 5 - Representación gráfica de los modelos de madurez
Fuente: Cobit 4.1

5.1 Ejemplos de modelo de madurez para procesos del modelo

Para poder definir el nivel de madurez de cada proceso, se deberá evaluar de forma independiente cada atributo, es decir se deberá encontrar la forma de poder medir de manera efectiva la capacidad de desarrollo de cada proceso.

Para el ejemplo detallado a continuación, se establece un cuestionario de preguntas asociadas a cada proceso. Las mismas están separadas por atributos, con lo cual para establecer un criterio de ponderación, se definen las siguientes premisas:

- De acuerdo a la figura 6 existe un promedio de la industria, cercano a 3 para cada proceso, con lo cual se dejara el valor de 3 para este ejemplo
- El valor asignado a cada pregunta es consecuente con los niveles de madurez definidos en la figura 7 es decir de 0 a 5.
- Para definir el nivel de atributos y del proceso en sí, se promediara sobre los valores asignados.

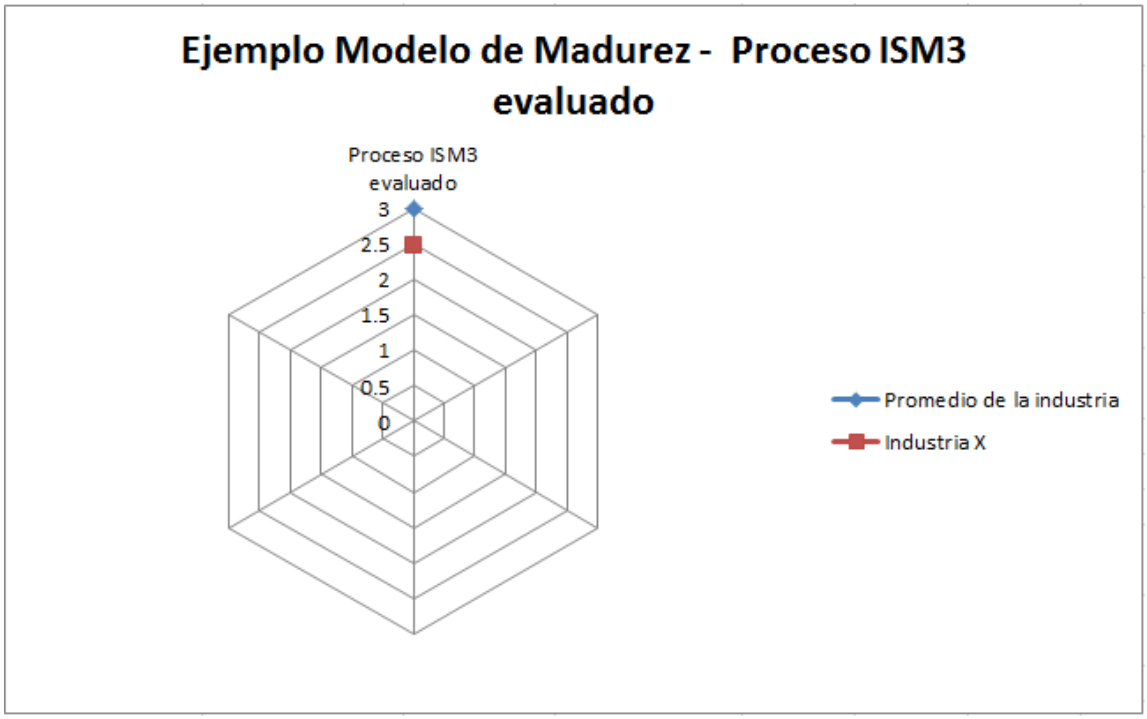


Figura 6 - Ejemplo Nivel de Madurez – Procesos ISM3 Evaluado

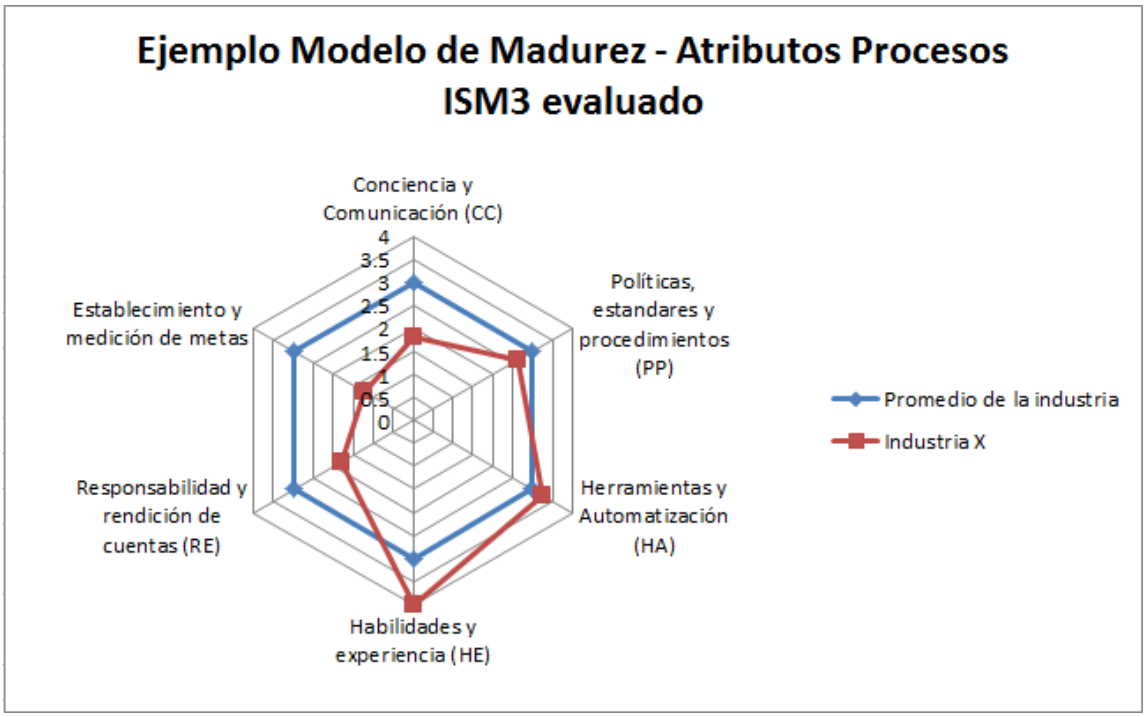


Figura 7 - Ejemplo Modelo de Madurez – Procesos ISM3

6 Conclusiones

La información como activo valioso para cualquier tipo de organización debe ser protegida contra amenazas que cada día son más sofisticadas y que intentan vulnerar controles débiles o mal implementados, para así poder tener acceso a datos restringidos o confidenciales. Es evidente que algunas empresas puede contar con las mejores herramientas tecnológicas a nivel de software y hardware que soportan las funciones operativas, pero muchas de ellas dejan a un lado la gestión de la Seguridad de la Información. Si no se cuenta con el apoyo desde el punto de vista estratégico de la organización, será muy difícil que un modelo de gestión de la Seguridad cumpla con el objetivo definido.

Caso contrario sería si la Alta dirección está comprometida, ya que servirá de soporte para que la gestión del área de Seguridad tenga elementos suficientes para abordar puntos frágiles y administrar tanto estratégicamente como operativamente, esto con el fin de disminuir vulnerabilidades y amenazas que puedan generar impacto sobre los activos de información. Implementar un modelo de Seguridad de la información servirá de base para gestionar la Seguridad, ayudara a las organizaciones a identifican los procesos claves que están ejecutando y que a su vez soportan activos críticos, o en un mayor nivel objetivos o metas de negocio, de esta forma se podrá fácilmente establecer controles, medir el desempeño del proceso y mejorar continuamente el mismo.

El modelo O-ISM3 establece elementos fundamentales para asumir este reto que tiene como fin la implementación de un modelo de seguridad, ya que establece todo el circuito de una manera detallada relacionando aspecto como: La descripción del proceso, definición de métricas, apoyo de otros frameworks, relación con otros procesos, metodologías o herramientas utilizadas, entre otros aspectos relevantes.

El reto esta desde el lado de las áreas de Seguridad ya que deberá brindar elementos suficientes a las áreas estratégicas para que este apoyo pueda ser lo suficientemente relevante, para que el concepto operativo haga parte de una serie de tareas funcionales, administradas y gestionadas de un manera eficiente.

7 Bibliografía

- [1] **ISM3**

http://www.iso27000.es/herramientas.html#section7a

Fecha de consulta: Julio de 2013

- [2] **SGSI**

http://www.iso27000.es/sgsi.html

Fecha de consulta: Julio de 2014

- [3] **Activo de Información**

http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

Fecha de consulta: Julio de 2014

- [4] **Proceso**

http://www.implementacionsig.com/index.php/interpretacion-de-la-norma-iso-9001/3-terminos-y-definiciones-iso-9001

Fecha de consulta: Julio de 2014

- [5] **Métricas**

http://www.unit.org.uy/misc/novedades/2008-06-12_Metricas_Unit.pdf

Fecha de consulta: Julio de 2014

- [6] **Modelo de Madurez**

http://blog.datknosys.com/2012/07/11/modelos-de-madurez-de-inteligencia-de-negocios-bi/

Fecha de consulta: Julio de 2014

- [7] **Matriz RACI**

http://itilv3.osiatis.es/diseno_servicios_TI/modelo_RACI.php

Fecha de consulta: Julio de 2014

- [8] **Gestión del Conocimiento**

http://itilv3.osiatis.es/transicion_servicios_TI/gestion_conocimiento.php

Fecha de consulta: Julio de 2014

- **ISO 27001**

http://www.iso27000.es/

Fecha de consulta: Julio de 2014

- **Cobit 4.1**

Framework para el Gobierno y control de TI

ISACA – Descarga Gratuita

http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

Fecha de consulta: Julio de 2014

- **Cobit5**

Framework para el Gobierno y la Gestión de TI de la empresa

ISACA - Descarga gratuita

http://www.isaca.org/COBIT/Pages/Product-Family.aspx

Fecha de consulta: Julio de 2014

- **ITIL**

http://itilv3.osiatis.es/

Fecha de consulta: Julio de 2014

- **O- ISM3**

Open Information Security Management Maturity Model

Aceituno, Vicente, 2011

http://www.opengroup.org/news/press/open-group-releases-maturity-model-information-security-management

Fecha de consulta: Julio de 2014

- **NIST – 800-55**

http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Fecha de Consulta: Julio de 2014