

GUIA METODOLOGICA

Implantación de un SGSI

SEGURIDAD DE LA INFORMACIÓN

Versión 1.0 – 2012

Este documento ha sido elaborado por AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento)

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento así como hacer obras derivadas, siempre y cuando tengan en cuenta citar la obra de forma específica y no utilizar esta obra para fines comerciales. Toda obra derivada de esta deberá ser generada con estas mismas condiciones.

"la seguridad de la información es un asunto de personas, procesos y tecnología"

Bruce Schneier

Tabla de Contenido

Tabla de Contenido	5
Glosario y Referencias	7
Glosario.....	7
Referencias.....	10
Abreviaturas y Siglas	10
Bibliografía recomendada	11
Introducción	13
Objetivo y alcance.....	14
El Sistema de Gestión de Seguridad de la Información.....	14
Principios	14
Beneficios	15
Marco normativo	16
Ley 18331: Protección de datos personales y acción de habeas data	16
Ley 18381: Acceso a la información pública	17
Decreto 452/009.....	17
Resolución Consejo Directivo Honorario	18
Estructura de trabajo.....	19
Responsable de Seguridad de la Información (RSI).....	19
Comité de Seguridad de la Información (CSI)	20
Introducción	25
Fase 1: Diagnostico	26
Objetivo.....	26

Descripción	26
Recomendaciones.....	28
Fase 2: Planificación.....	29
Objetivo.....	29
Descripción	29
Fase 3: Implementación.....	31
Objetivo.....	31
Fase 4: Evaluación y monitoreo	32
Objetivo.....	32
Anexo I.....	36
Inventario de activos	36
Análisis de riesgos	40
Plan de Seguridad de la Información	41
Indicadores	42

Glosario y Referencias

Glosario

A

Acceso a la información

Contacto directo con la información alojada en los repositorios del CERTuy.

Activos de información

Son aquellos datos o información que tienen valor para una organización. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Activos de información críticos del Estado

Son aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Alerta

Es cualquier vulnerabilidad o amenaza que pueda afectar determinado activo.

Alerta relevante

Aquella alerta que puede involucrar a activos críticos de la Comunidad Objetivo y que en caso de explotarse, podría implicar un daño significativo para el activo en cuestión.

D

Destrucción de información

Se entiende por destrucción al proceso irreversible de dejar la información no disponible.

E

Evento de seguridad informática

Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad.

[Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

G

Gestión de Incidentes:

Es el conjunto de acciones y procesos tendientes a brindar a las organizaciones de la Comunidad Objetivo fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios.

I

Impacto significativo

Serán impactos significativos para la comunidad:

- Aquellos que puedan provocar riesgo de vida a personas
- Aquellos que afecten levemente a más de 50.000 ciudadanos
- Aquellos que provoquen al Estado Uruguayo una pérdida económica significativa
- Aquellos que deterioren la imagen de un organismo estatal

Incidente de seguridad de la información

Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

[ISO/IEC 27035:2011]

Incidente de seguridad informática

Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

[Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Información sensible

Se denominará genéricamente como información sensible, a aquella información clasificada como confidencial, reservada, reservada de uso de la comunidad o secreta.

N

Negocio

Se entiende por negocio el objetivo o conjunto de objetivos que persigue el organismo, como por ejemplo los servicios ofrecidos, y prestaciones en general.

P

Principales actores:

Son aquellas organizaciones públicas o privadas que gestionen, participen o controlen un proceso crítico o que por su actividad deban gestionar la disponibilidad, confidencialidad o integridad de algún activo de información crítico.

Procesos críticos:

Son aquellos procesos que dan soporte sustantivo a los servicios previamente identificados como esenciales, y cuya interrupción degrada significativamente la capacidad del sector de dar correctas respuestas a la comunidad. Los mismos pueden ser gestionados en una o varias instituciones.

Propietarios de activos de información

Son los responsables de la clasificación conforme a los procedimientos establecidos, el mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias.

S

Sistema informático

Los ordenadores y redes de comunicación electrónica así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

[Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Referencias

[1] Ley 18331: Protección de datos personales y acción de habeas data

<http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331>

[2] Ley 18381: Acceso a la información pública

<http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18381>

[3] Decreto 452/009

http://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto_n%C2%B0_452_009_de_28_de_setiembre_de_2009.html

[4] Resolución 62/010

http://www.agesic.gub.uy/innovaportal/v/1224/1/agesic/resolucion_cdh_62_010_de_13_de_octubre_de_2010.html?menuderecho=1

[5] Guía de actividades del Responsable de Seguridad de la Información, AGESIC.

Abreviaturas y Siglas

RSI Responsable de Seguridad de la Información

CSI Comité de Seguridad de la Información

CDH Consejo Directivo Honorario

SGSI Sistema de Gestión de Seguridad de la Información

AGESIC Agencia de Gobierno Electrónico y la Sociedad de la Información y del Conocimiento

ISO

UE Unidad Ejecutora

Bibliografía recomendada

Compendio digital de normas: Seguridad de la Seguridad de la Información [Recurso electrónico] / UNIT. – [Versión] 0.1. Montevideo: UNIT, [2005]. 1 disco óptico electrónico (CD-ROM).

UNIT- ISO/IEC TR 18044: 2004- Documentos- Tecnologías de la Información. Técnicas de seguridad: Gestión de incidentes de seguridad de la Información. / UNIT, ISO. // Montevideo: UNIT, 2004.

UNIT-ISO/IEC 27000: 2009- Documentos- Tecnologías de la Información. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información- Visión general y vocabulario. / UNIT, ISO. // Montevideo: UNIT, 2009.

UNIT- ISO/IEC 27001: 2005- Documentos- Tecnologías de la Información. Técnicas de seguridad: Sistema de gestión de seguridad de la información. Requisitos. / UNIT, ISO. // Montevideo: UNIT, 2006.

UNIT-ISO/IEC 27002: 2005- Documentos- Tecnologías de la Información: Códigos de buenas prácticas para la gestión de la Seguridad de la Información. / UNIT, ISO. // Montevideo: UNIT, 2005.

Capítulo I

Introducción

Introducción

Habitualmente, en lo que refiere a seguridad, se piensa en garantizar la seguridad de los sistemas informáticos; al adoptar normas como la ISO 27001 u otras normas técnicas o estándares, como modelos de desarrollo de la seguridad, tenemos que derribar viejos paradigmas. Pasamos así de un modelo basado en la seguridad informática a un sistema basado en la seguridad de la información.

Para aquellos que no están familiarizados con el modelo ISO 27001, esta diferencia puede parecer trivial; aunque nada más lejos de la realidad. Al cambiar el foco hacia la información en sentido amplio, nos vemos obligados a contemplar aspectos relacionados con la seguridad que escapan a las consideraciones únicamente desde una óptica informática, para trascender a un universo completo donde la información radica en todo medio de conservación imaginable, incluso el biológico.

En este nuevo paradigma, hemos ampliado la visión, pero sigue incluyendo los aspectos informáticos clásicos como los controles perimetrales, la vulnerabilidad, la detección de intrusos en los sistemas, pero ahora, además, se debe garantizar que el personal sea capaz de gestionar la información de la organización de una forma segura, independientemente del formato o soporte en el que se encuentra. Configurar equipos o instalar productos tiene una dimensión controlable desde un departamento de sistemas, lograr que todo el personal del organismo sea consciente de la importancia de la seguridad de la información y siga los procedimientos y las normas para garantizar esta seguridad, es más complejo.

A continuación se describen los lineamientos de cómo implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Es importante destacar que cuando el organismo se embarca en el proceso de implantación de un SGSI se van a designar personas, se van a modificar procesos que son de impacto para el Organismo, se van a implantar controles, se van a cambiar un muchos casos las modalidades de trabajo; ante estas situaciones de cambio resulta fundamental que las personas que toman las decisiones dentro del Organismo no solo estén enteradas y convenidas de que esto es importante, sino que será imprescindible su apoyo para llevar adelante los cambios. Por tanto, resulta imprescindible el apoyo de la alta dirección para la implantación y mantenimiento de un SGSI.

Objetivo y alcance

El objetivo de este documento es brindar los primeros lineamientos para que un organismo pueda comenzar con la implantación de un SGSI.

Esta guía tiene como finalidad ayudar al Responsable de Seguridad de la Información en la definición de un SGSI para su organismo, y bitácora de trabajo de lo que serán los primeros pasos de la metodología.

El Sistema de Gestión de Seguridad de la Información

Principios

El Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información.

- **Confidencialidad:** garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, considera la ampliación de estos conceptos en otros:

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **No duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se

registren múltiples transacciones con el objetivo de generar instancias fraudulentas (falsas).

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo y la información de éste.
- **Confiabilidad:** es decir, que la información generada, almacenada o transmitida sea cierta y por tanto confiable para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Beneficios

Control interno

Existencia de Control Interno y dotar de un Marco de referencia con el objetivo de lograr mayor eficiencia en las operaciones; tener mayor confiabilidad de la Información Económico – Financiera, así como operativa; y adecuarse al cumplimiento de las normas y regulaciones aplicables.

Reducción de costos

(Gestionar los riesgos) La implantación de un SGSI incide directamente sobre los gastos económicos del Organismo en relación a una ineficiente gestión de la seguridad. En el corto plazo pueden existir costos vinculados a la implantación de controles, pero estos deben ser vistos como inversiones a mediano y largo plazo. La implementación de dichos controles suelen redundar en mejoras.

Los beneficios surgen de, por ejemplo, la reducción de primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados, o evitando indemnizar a los usuarios por malas gestiones.

Continuidad del negocio¹

(Disponibilidad de la información) Con un SGSI en marcha se evitan interrupciones en los servicios ofrecidos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que el organismo ofrece. Esto en cuanto a la actividad cotidiana, pero también se está preparado para recuperarse ante incidentes más o menos

¹ Se entiende por negocio el objetivo o conjunto de objetivos que persigue el organismo, como por ejemplo los servicios ofrecidos, y prestaciones en general.

graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el mismo a largo plazo.

Mantener y mejorar la imagen

(Credibilidad y confianza) Los usuarios percibirán al organismo como una entidad responsable, comprometida con la mejora de sus procesos, productos y servicios. Debido a la exposición de cualquier organismo a un fallo de seguridad que pueda hacer pública información reservada o confidencial, un SGSI implantado coloca al Organismo en una posición de reconocimiento ante la ciudadanía y sus pares. Una imagen consolidada de confianza, facilita la gestión general y habilita nuevas posibilidades para la toma de decisiones.

Cumplimiento legal y reglamentario

Día a día el marco normativo referido a seguridad de la información se afianza y consolida, en este contexto contamos con normas como: ley de protección de datos personales y acción de habeas data, y ley de acceso a la información pública.

Un SGSI permite dar cumplimiento al marco normativo con mayor rapidez y eficiencia. Un logro importante para todo Organismo.

Marco normativo

Ley 18331: Protección de datos personales y acción de habeas data

Esta ley establece que se deberán registrar todas las bases de datos que contenga información de personas físicas y jurídicas.

Según cita la ley:

“Artículo 2°. Ámbito subjetivo.- El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda.

Artículo 3°. Ámbito objetivo.- El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

No será de aplicación a las siguientes bases de datos:

- a. A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- b. Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
- c. A las bases de datos creadas y reguladas por leyes especiales.” [1]

Ley 18381: Acceso a la información pública

Esta ley establece que toda información producida por el organismo deberá ser pública, salvo que entre en las categorías de confidencia, reservada o secreta.

Según cita la ley:

“Artículo 1°. (Objeto de la ley).- La presente ley tiene por objeto promover la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública.

Artículo 2°. (Alcance).- Se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales.

Artículo 3°. (Derecho de acceso a la información pública).- El acceso a la información pública es un derecho de todas las personas, sin discriminación por razón de nacionalidad o carácter del solicitante, y que se ejerce sin necesidad de justificar las razones por las que se solicita la información.” [2]

Decreto 452/009

Este decreto [3] establece que todas las unidades ejecutoras deben adoptar una política de seguridad de la información, tomando como base la propuesta en dicho decreto. Además exhorta a los gobiernos departamentales, entes

autónomos, servicios descentralizados y demás órganos del estado a adoptar las disposiciones establecidas por el decreto.

Política de seguridad de la información

En líneas generales establece que se debe:

- Tener objetivos anuales en seguridad de la información.
- Implementar controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura, para asegurar los objetivos.
- Designar un responsable de seguridad de la información.
- Elaborar una **política de gestión de incidentes**
- Elaborar una **política de gestión de riesgos**
- Concientizar al personal.
- Tener un plan de continuidad del negocio.

Resolución Consejo Directivo Honorario

La resolución 62/010[4] del Consejo Directivo Honorario de AGESIC establece que AGESIC podrá fiscalizar el cumplimiento de decreto 452/009, y podrá apercibir a los organismos que no cumplan dicha normativa.

Estructura de trabajo

Si bien la estructura organizacional en materia seguridad de la información no es objeto de esta guía, sí vamos a definir las 2 figuras o roles que son base para el trabajo en seguridad de la información estableciendo las responsabilidades que cada uno debería tener. No obstante queda abierto a modificaciones de cada organismo de manera que se adapte a cada realidad particular.

Responsable de Seguridad de la Información (RSI)

Se trata de una figura cuya labor es garantizar la implementación de políticas, medidas y acciones, que contribuyan a la salvaguarda de la información del Organismo u oficina pública, en los contextos que sean pertinentes según sea ésta pública, reservada o confidencial.

Según lo recomienda la Guía de actividades del RSI [5], dentro de sus principales actividades se encuentra:

- a. Verificar la alineación de la seguridad de la información con los objetivos estratégicos del Organismo.
- b. Guiar, implementar, mantener y documentar el Sistema de Gestión de Seguridad de la Información del Organismo.
- c. Revisar en forma periódica los documentos y controles del Sistema de Gestión de Seguridad de la Información del Organismo.
- d. Coordinar con los "propietarios" de los procesos y activos de información, la alineación con la seguridad de la información definida por el Organismo.
- e. Asegurar que la implementación de los controles de seguridad de la información es coordinada en todo el Organismo.
- f. Verificar la falta o superposición de controles en seguridad de la información.

- g. Desarrollar métricas y métodos que permitan monitorear las actividades de seguridad de la información, y verificar la eficiencia y eficacia de los controles.
- h. Promover la difusión, concientización, educación y la formación en seguridad de la información en el Organismo.
- i. Promover el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.
- j. Promover el cumplimiento de las políticas y documentos relacionados del Sistema de Gestión de Seguridad de la Información del Organismo.
- k. Identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas.
- l. Evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad de la información y las acciones recomendadas en respuesta a los mismos.
- m. Colaborar con el equipo responsable por la Gestión de Incidentes de Seguridad de la Información del Organismo.
- n. Colaborar con el equipo responsable por la Gestión del Riesgo de Seguridad de la Información del Organismo.
- o. Colaborar con el equipo responsable por la definición e implementación del Plan de Continuidad del Negocio del Organismo.

Es importante que esta persona cuente con el aval y respeto de todas las direcciones del organismo, por esto a la hora de elegir a la persona que lleve adelante este rol es necesario que sea elegido en consenso.

Cualidades como: liderazgo, capacidad para lograr acuerdos, aceptación de sus pares, poder de gestión; son fundamentales para llevar con éxito la tarea de RSI.

Comité de Seguridad de la Información (CSI)

El comité de seguridad de la información deberá estar formado por representantes de todos los directores, si el comité está formado a nivel del inciso, corresponde a los directores de la unidades ejecutoras, si es una unidad

ejecutora, entonces serán los directores de áreas. Cuando el CSI se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación del RSI.

Este comité tendrá reuniones que, se recomienda, no deberán ser más allá de mensuales. Se espera que en las primeras instancias de reunión del comité, puedan estar los propios directores de manera de estimular la aprobación de políticas y normativas en relación a la Seguridad de la Información; luego las reuniones se irán enfocando más a la planificación estratégica y gestión de aspectos vinculados a la seguridad, por lo que se dará participación a los representantes de las respectivas direcciones involucradas.

El CSI tendrá como principales funciones:

- a. Estudio de la Política de Seguridad de la Información, previo a su aprobación.
- b. Proponer las responsabilidades generales en materia de seguridad de la información.
- c. Brindar lineamientos estratégicos al Responsable de Seguridad de la información.
- d. Apoyar y aprobar aquellas iniciativas que incrementen la seguridad de la información.
- e. Garantizar que la seguridad sea parte del proceso de planificación de la información.
- f. Promover la difusión y apoyo a la seguridad de la información dentro de las unidades ejecutoras.

Capítulo II

Fases de implantación

Introducción

Para comenzar a trabajar en seguridad de la información lo primero que se deberá realizar es la definición de las estructuras adecuadas para que esto pueda tener sustento a largo plazo.

Por estructura se entiende:

- creación del comité de seguridad de la información, el mismo debe estar integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- designación del responsable de seguridad de la información, que cumplirá la función de supervisar el cumplimiento de la Política de Seguridad de la Información y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.
- aprobación de políticas de alto nivel (como mínimo se deberán aprobar las políticas de Seguridad de la Información, Gestión de Riesgos y Gestión de Incidentes) por parte de la dirección, etc.

Lo que se propone en la presente guía metodológica es la aplicación de 4 fases para ordenar el trabajo, y facilitar la puesta en marcha de un sistema de gestión de seguridad de la información. A continuación se presentan las 4 fases sugeridas y los objetivos que cada una de ellas persigue.



Fase 1: Diagnostico

Objetivo

Diagnosticar la situación de seguridad de la información, poniendo énfasis en identificar adecuadamente los activos de información vinculados a sus procesos, así como los riesgos asociados a dichos activos.

Descripción

La fase de diagnóstico es fundamental ya que entrega los lineamientos para el trabajo a desarrollar en las fases siguientes.

Desde el punto de vista de Seguridad de la Información, se enfatiza la capacidad de generar valor mediante el uso de políticas, estándares, procedimientos y buenas prácticas de seguridad que, en complemento con las TIC, conforman un sistema de gestión administrativo.

Sin embargo, el objetivo no es la incorporación de dichas tecnologías a la normativa interna, sino la mejora de la gestión de los organismos a través de ellas. En este sentido, es indispensable que los servicios determinen si sus áreas y divisiones requieren mejoras antes de intervenir en sus procesos, para no generar actividades de control que sean innecesarias, utilizando recursos que pueden aprovecharse en necesidades más urgentes en el organismo.

Es importante destacar que uno de los aspectos relevantes para la aprobación de esta fase es la identificación de los activos de información asociados a los procesos de provisión de bienes y servicios, y los riesgos a los que se encuentran sometidos, a fin de poder definir las medidas requeridas para su mitigación.

Es necesario que el RSI, como también todos los funcionarios que tengan participación en el llenado del inventario de activos, cumpla con la totalidad de los pasos necesarios y requisitos técnicos, con el fin de lograr y asegurar un cumplimiento satisfactorio de la fase de Diagnóstico.

A los efectos del Diagnóstico requerido en el sistema, se ha dispuesto una planilla electrónica de “Identificación de Activos”, que se presenta en detalle en el ANEXO I.

Inventario de activos de información

El Diagnóstico tiene foco en la correcta identificación de los activos de información del organismo, y para ello es recomendable identificar primeramente los procesos de negocio.

La realización de cada uno de los procesos involucra activos de información específicos, en sus diversos tipos y formatos.

Dichos activos de información son los que se requiere listar y caracterizar en la hoja “Inventario de Activos”, de la planilla de Identificación de Activos.

	A	B	C	D	E	F	G	H	I	J	K
1	Organismo/UE:										
2	Nombre del Proceso/Subproceso:										
3	ACTIVOS DE INFORMACION IDENTIFICADOS								VALORACION DE LOS ACTIVOS		
4	Activo	Tipo	Grupo	Descripción	Utilización	Responsable/Dueño	Soporte	Clasificación	Disp.	Int.	Conf.
5											
6											
7											
8											
9											
10											

Análisis de riesgos

Una vez identificados los activos de información se requiere identificar y caracterizar los riesgos que amenazan a dichos activos, cuantificando el nivel de severidad de riesgo y el tratamiento sugerido. Dichos riesgos se deben listar y caracterizar en la hoja “Análisis de Riesgos” de la planilla de Identificación de Activos.

Esta hoja está dividida en dos partes, por un lado, el análisis de riesgo actual; este análisis se realiza en base a la exposición y al impacto sobre el organismo resultando en un “número de riesgo”, la exposición se calcula en base a las amenazas y vulnerabilidades.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Grupo	Amenazas	Descripción	Prob.	Controles	Vulnerabilidades	Nivel Vul.	Exp.	D	I	C	Impacto	Riesgo Actual
2	Bases de datos	Acceso no autorizado	* Usuario interno o externo que logra ingresar a un sistema o área restringida. * Esta amenaza puede ser lógica o física.	Baja	Físico: las bases de datos están en datacenter con control de acceso Contratos de confidencialidad	No hay control sobre el otorgamiento de permisos a las base de datos de producción.	Media	Baja	x	x	x	Medio-Alto	4
3	Bases de datos	Incumplimiento de requisitos legales, regulatorios o contractuales	* Software, Hardware, servicios o personas que estén incumpliendo de alguna manera requisitos legales, regulatorios o contractuales establecidos en la empresa.	Media	Las bases de datos con datos personales han sido registradas.		Alta	Alta	x		x	Medio	5

Por otro lado, tenemos el riesgo residual; esto refiere al riesgo que se obtiene de aplicar los tratamientos sugeridos para los riesgos actuales.

	A	B	N	O	P	Q	R	S	T
1	Grupo	Amenazas	Tratamiento	Controles	Nueva Prob.	Nuevo Nivel Vul.	Nuevo Exp.	Nuevo Impacto	Riesgo Residual
2	Bases de datos	Acceso no autorizado					Baja		#N/A
3	Bases de datos	Incumplimiento de requisitos legales, regulatorios o contractuales					Baja		#N/A

Recomendaciones

Para comenzar a trabajar en la implantación de un SGSI, y a la hora de elegir alcance para la fase de Diagnóstico se recomienda escoger los activos de información vinculados a un proceso o departamento del organismo que no sea crítico, pero que sí tenga relevancia para el mismo.

Esto es fundamental principalmente si el equipo de trabajo aún no tiene experiencia en la metodología, permitiendo a su vez realizar los ajustes de la misma acorde a la cultura del organismo.

Luego de ajustada la metodología, se espera que se vayan incorporando procesos a la fase de Diagnóstico, y esto incluye los procesos críticos del organismo.

Fase 2: Planificación

Objetivo

- Definir el Plan de Seguridad de la Información (PSI) del organismo, considerando los resultados del diagnóstico realizado en la fase 1. Este plan deberá estar aprobado por el CSI y tendrá que incluir el tratamiento y monitoreo para todos los riesgos críticos identificados; la identificación de los productos necesarios para el debido tratamiento de los riesgos; los responsables para cada producto y finalmente la definición del porcentaje de cumplimiento que se espera alcanzar durante el año.
- Plan de Mitigación de Riesgos, que defina los riesgos asociados al Plan de Seguridad de la Información y sus acciones para resolverlos.
- Elaborar el Programa de Trabajo Anual para implementar el Plan de Seguridad de la Información definido, que incluya hitos, cronograma, plazos y responsables, y las acciones orientadas a difusión, capacitación y sensibilización a todos los funcionarios del programa de trabajo y sus productos.

Descripción

En esta fase se definen los objetivos de la implementación de soluciones y la mitigación de los riesgos identificados en la fase de Diagnóstico, diseñando un completo programa de trabajo que permita alcanzar dichos objetivos en los plazos establecidos. Además, permite la coordinación de esfuerzos y recursos al interior de los organismos garantizando el éxito de las iniciativas.

En esta fase ya se han tomado las decisiones respecto del diagnóstico elaborado en la fase anterior, en el cual se establecieron, las prioridades según las necesidades del organismo.

El resultado de la información levantada en la fase de Diagnóstico, será la guía para destinar los recursos disponibles y establecer los requerimientos adicionales.

Es importante que esta etapa se desarrolle con la debida antelación, de modo que sea consistente con el proceso de planificación presupuestaria.

Planificación

En el caso particular del SGSI, los proyectos o actividades que se incluyen en esta fase adquieren la calidad de compromisos, a los cuales se les realizará un seguimiento que concluye en la fase de Evaluación y monitoreo.

Para que el organismo pueda cumplir tales compromisos debe trazar una ruta que organice el trabajo, que incluya elementos de planificación de tareas y funciones, lo que garantizará el éxito de esta fase.

Para poder establecer un Plan de Seguridad de la Información, se deberán tener en cuenta los siguientes elementos:

- Política de seguridad de la información.
- Objetivos estratégicos para la seguridad de la información.
- Resultado de la fase de Diagnóstico: análisis de riesgos.

Creación del Plan de Seguridad de la Información

Una vez realizada la fase de Diagnóstico se obtiene el inventario de activos con su correspondiente análisis de riesgo, y los productos y controles necesarios para mitigar los riesgos potenciales.

Para cada producto definido será necesario establecer en un plan de trabajo las actividades que se requiere para lograr su implementación. En la hoja “Plan Seguridad Información” de la planilla “Identificación de activos” se presenta

	A	B	C	D	E	F	G	H
1								
2		Producto esperado	Responsable del producto	PROGRAMA DE TRABAJO			Recursos humanos y materiales	Costos
3			Actividad	Fecha de inicio	Fecha término	Responsable de la actividad		
4		<Producto>						
5		<Actividad>						
6		<Actividad>						
7		<Actividad>						
8		<Producto>						
9		<Actividad>						
10		<Actividad>						
11		<Actividad>						

una estructura del plan de trabajo.

Además se deberán definir para cada producto el o los indicadores que se utilizarán para su evaluación y seguimiento. En la hoja “Indicadores” de la planilla “Identificación de activos” se presenta una estructura para el registro de indicadores.

	A	B	C	D	E	F	G	H	I
1									
2		Producto asociado	Nombre del indicador	Fórmula de cálculo	Fecha de inicio de la medición	Frecuencia de la medición	Meta	Medios de verificación	Observaciones
3									
4									
5									
6									

Fase 3: Implementación

Objetivo

- Implementar el programa de trabajo anual.
- Controlar los resultados de la implementación del programa de trabajo anual.
- Medición de los indicadores.

Descripción

Implementar el programa de trabajo anual

Ejecutar las actividades mencionadas en el programa de trabajo anual definido en la fase anterior, de acuerdo a lo establecido en el Plan de Seguridad de la Información y el porcentaje de cumplimiento comprometido.

Controlar los resultados de la implementación del programa de trabajo anual

Registrar y controlar los resultados de la implementación del programa de trabajo anual considerando actividades, dificultades, implementación del plan de mitigación de riesgos asociados a cada proyecto o iniciativa, las acciones de difusión, sensibilización y capacitación, y las modificaciones realizadas según lo programado.

Medición de los indicadores

Comenzar con la medición de los indicadores establecidos en el programa de trabajo anual. Este objetivo es muy importante ya que de los resultados que devuelvan los indicadores se formularán las metas para el siguiente año (periodo).

Para mayor detalle sobre indicadores ver Anexo II.

Fase 4: Evaluación y monitoreo

Objetivo

- Evaluar los resultados del Plan de Seguridad de la Información.
- Diseñar el programa de seguimiento.
- Difundir a los funcionarios el resultado de la evaluación.
- Mejora continua del SGSI.

Descripción

Evaluar los resultados del Plan de Seguridad de la Información

Evaluar los resultados de la implementación del Plan de Seguridad de la Información y Programa de Trabajo Anual, y formular recomendaciones de mejora.

La evaluación del sistema de gestión de seguridad de la información debe ser conocida y valorada por el comité de seguridad de la información. Las conclusiones y recomendaciones que realice el comité deberán quedar reflejadas en el programa de seguimiento de esta fase.

Diseñar el programa de seguimiento

Las recomendaciones realizadas en la evaluación que queda como resultado del punto anterior, es el insumo principal para la elaboración del programa de seguimiento.

Este programa de seguimiento tiene como objetivo realizar y dar seguimiento a las recomendaciones surgidas de la evaluación. Las mismas deberán ser realizadas en el año corriente, siendo excepcional el pasarlas como actividades del año próximo.

Difundir a los funcionarios el resultado de la evaluación

Difundir a los funcionarios los resultados de la evaluación del Plan de Seguridad de la Información y del Programa de Trabajo Anual es fundamental para mantener vivo el interés en la seguridad de la información y mostrar que se está trabajando en el tema.

Este tipo de actividad no debe confundirse con la difusión y concientización en seguridad de la información.

Mejora continua del SGSI

Implementar los compromisos establecidos en el Programa de Seguimiento, considerando plazos y responsables para superar debilidades detectadas.

Se deberán establecer un conjunto de medidas que permitan sostener y mejorar el SGSI, más allá del proceso de implementación. Para lograr cumplir con este objetivo, se deberá proponer un sistema de control y mejora continua, que al menos establezca una planificación que considere las revisiones regulares del SGSI. También se debe incluir:

- la revisión de los indicadores y metas propuestas;
- las medidas de mejora a partir de los resultados;
- la aprobación de dichas medidas por parte del comité de seguridad de la información;
- la actualización de inventario de activos y

- la correspondiente gestión de riesgo.

Capítulo III

Anexos

Anexo I

	A	B	C	D	E	F	G	H	I	J	K
1	Organismo/UE:										
2	Nombre del Proceso/Subproceso:										
3	ACTIVOS DE INFORMACION IDENTIFICADOS								VALORACION DE LOS ACTIVOS		
4	Activo	Tipo	Grupo	Descripción	Ubicación	Responsable/Dueño	Soporte	Clasificación	Disp.	Int.	Conf.
5											
6											
7											
8											
9											
10											

Inventario de activos

Descripción de los campos:

Organismo/UE: Nombre del organismo o unidad ejecutora para el cual se esté realizando la identificación de activos.

Nombre del Proceso: Corresponde al nombre del proceso de negocio al cual pertenecen los activos de información incluidos en el inventario.

Subproceso: Son aquellos subprocesos en los que puede estar dividido el proceso transversal mencionado anteriormente, dependiendo de la complejidad del mismo.

ACTIVOS DE INFORMACION IDENTIFICADOS

Activo: Nombre del activo de información, en este campo debe incluirse todos los activos de información identificados para la fase, independientemente de su medio de soporte y sus características.

Tipo: Clasificación o categorización del activo. Esta puede ser: Persona, Software, Base de datos, Hardware, Servicio, Documentación impresa, Documentación digital, etc.

Grupo: Categorías o agrupaciones dentro de un mismo tipo. Por ejemplo: Tipo=Base de datos; Grupo=Pruebas.

Descripción: Descripción u observaciones del activo inventariado.

Ubicación: Corresponde al lugar físico donde se encuentra el activo, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad en las que se encuentra el activo.

Responsable: Corresponde al nombre y al cargo de la persona responsable del activo. El dueño del activo puede no tener derechos de propiedad sobre el activo, pero tiene responsabilidad sobre su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El dueño del activo a menudo es la persona más apropiada para determinar el valor que el activo tiene para el organismo².

Soporte: Corresponde al medio en el cual se encuentra registrado el activo, este puede ser: Papel, Digital o Base de datos.

Clasificación: Pública, Confidencial, Reservada o Secreta según los criterios establecidos en la ley de acceso a la información pública.

VALORACION DE LOS ACTIVOS

Disponibilidad: Valor establecido según tabla que se presenta a continuación.

Valor	Concepto
-------	----------

² ISO 27005 Pto 8.2.1.2

Bajo	Refiere a toda la información, medios de procesamiento de información y recursos donde la disponibilidad no es crítica y es suficiente para este activo el estar disponible dentro de 1 semana o más .
Medio	Refiere a toda la información, medios, recursos, que deberían estar disponibles dentro de un día , y la no disponibilidad del activo ocasionaría un impacto menor al negocio.
Medio-Alto	Refiere a toda la información, medios, recursos, que deberían estar disponibles dentro de algunas horas , y su no disponibilidad ocasionará un impacto notable para el negocio.
Alto	Refiere a toda la información, medios, recursos, que deberían estar disponibles en todo momento , y su no disponibilidad ocasionaría un impacto importante para el negocio.

Integridad: Valor establecido según tabla que se presenta a continuación.

Valor	Concepto
Bajo	Refiere a toda la información, medios de procesamiento de información y recursos donde la pérdida de integridad no tiene influencia, o influencia negativa en los negocios de la empresa.
Medio	Refiere a toda la información, medios, recursos, donde la integridad no es muy importante, pero debería ser mantenida. Para este activo, la pérdida de integridad tiene cierta influencia menor en el negocio de la empresa.
Medio-Alto	Refiere a toda la información, medios, recursos, donde la integridad es importante y debería ser mantenida. Para este activo la pérdida de integridad tiene influencia notable en el negocio y se debería evitar.
Alto	Refiere a toda la información, medios, recursos, donde la integridad es muy importante y debería ser mantenida bajo todas las circunstancias. Para este activo, la pérdida de integridad tiene una importante influencia negativa en el negocio, y se debería evitar.

Confidencialidad: Valor establecido según tabla que se presenta a continuación.

Valor	Concepto
Bajo	Refiere a información abierta, medios de procesamiento de información y recursos, información que esta libremente accesible por cualquiera. Por Ej. la información en el sitio Web de la empresa.
Medio	Refiere a toda la información, medios y recursos que es de uso Interno. Esto implica que el activo puede ser accesible por cualquier miembro de la empresa sin ninguna restricción, pero no debería ser accesible por cualquier otro externo. El impacto sobre la empresa seria medio.

Medio-Alto	Refiere a toda la información, medios, recursos, que está considerada de acceso restringido. Esto implica que el activo puede ser solamente accesible por miembros de la empresa, si son autorizados para eso. El impacto de que cualquiera no autorizado acceda a este activo sería notada y debería ser evitado.
Alto	Refiere a toda la información, medios, recursos, que este considerado como confidencial. Este activo debería ser solamente accesible con una autorización explícita. El impacto sería serio y debería ser evitado en todas las circunstancias.

Análisis de riesgos

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Grupo	Amenazas	Descripción	Prob.	Controles	Vulnerabilidades	Nivel Vul.	Exp.	D	I	C	Impacto	Riesgo Actual
2	Bases de datos	Acceso no autorizado	* Usuario interno o externo que logra ingresar a un sistema o área restringida. * Esta amenaza puede ser lógica o física.	Baja	Físico: las bases de datos están en datacenter con control de acceso Contratos de confidencialidad	No hay control sobre el otorgamiento de permisos a las base de datos de producción.	Media	Baja	x	x	x	Medio-Alto	4
3													

Descripción de campos:

Grupo: Grupo de activos a evaluar.

Amenazas: una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o a una organización.

Descripción: Descripción de la amenaza.

Prob.: probabilidad de ocurrencia de la amenaza.

Controles: Controles existentes que mitiguen la amenaza.

Vulnerabilidades: una debilidad de un activo o de un grupo de activos que puede ser explotada por una o más amenazas.

Nivel Vul.: grado de afectación de la vulnerabilidad.

Exp.: Grado de exposición; esto refleja que tan expuesto está el activo ante el “mundo” en base a las amenazas y vulnerabilidades que tiene.

D: Marcar con “x” si la amenaza afecta la disponibilidad de la información.

I: Marcar con “x” si la amenaza afecta la integridad de la información.

C: Marcar con “x” si la amenaza afecta la confidencialidad de la información.

Impacto: Valoración máxima asignada a Disponibilidad, Integridad o Confidencialidad dentro del grupo de activos referenciado. Pasa saber este valor se debe consultar la hoja “Inventario de Activos”.

Riesgo Actual: Valor asignado según la siguiente tabla, teniendo en cuenta la Exposición y el Impacto del grupo de activos.

MATRIZ DE RIESGOS					
Exposición → Impacto	Muy baja	Baja	Media	Alta	Muy Alta
No Aplica	0	0	0	0	0
Bajo	1	2	3	4	5
Medio	2	3	4	5	6
Medio-Alto	3	4	5	6	7
Alto	4	5	6	7	8

Tratamiento: Acciones o controles sugeridos para mitigar la amenaza.

Plan de Seguridad de la Información

	A	B	C	D	E	F	G	H
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

Descripción de campos:

Producto esperado: corresponde a cada tratamiento (control) identificado en la hoja de “Análisis de riesgos”.

Responsable del producto: nombre y cargo de la persona responsable de la implementación del producto.

Actividad: secuencia de actividades que el organismo debe realizar para la obtención del producto.

Fecha de inicio: corresponde a la fecha de inicio de la actividad.

Fecha de fin: corresponde a la fecha de fin prevista para la actividad.

Responsable de la actividad: nombre y cargo de la persona responsable de la realizar la actividad.

Recursos humanos y materiales: listado de recursos humanos y materiales necesario para obtener el producto o actividad.

Costos: costos previstos para la concreción del producto o actividad.

Indicadores

	A	B	C	D	E	F	G	H	I
1									
2		Producto asociado	Nombre del indicador	Fórmula de cálculo	Fecha de inicio de la medición	Frecuencia de la medición	Meta	Medios de verificación	Observaciones
3									
4									
5									
6									

Descripción de campos:

Producto asociado: identificación del producto que será evaluado con el respectivo indicador.

Nombre del indicador: descripción breve que da cuenta del objetivo del indicador.

Fórmula de cálculo: expresión matemática que permite cuantificar el nivel o magnitud que alcanza el indicador (si corresponde).

Fecha de inicio de la medición: fecha en la cual se comienza a realizar las mediciones que requiere el indicador.

Frecuencia de la medición: corresponde a la periodicidad establecida para la medición del indicador.

Meta: compromiso a alcanzar respecto del valor del indicador obtenido el año anterior.

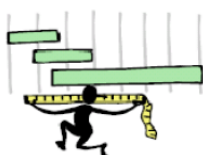
Medios de verificación: son los mecanismos de sistematización de la información que contienen el detalle requerido para la medición de los indicadores y a su vez, permiten verificar los valores informados en cada cifra del indicador, no solo el valor final.

Observaciones: notas o precisiones de alguna de las variables del indicador.

Anexo II

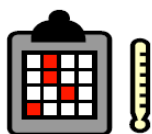
Indicadores

Medidas e indicadores



MEDIDA

Número o categoría asignada a un atributo de una entidad mediante una medición [ISO 14598-1:1999]



MÉTRICA

Interpretación de la medida.



INDICADOR

Provee una visión en cuanto al logro de objetivos.

¿Qué medir?

Una medida, por sí misma, no es una métrica. Debe incluirse también el factor tiempo; tampoco la métrica sola es la respuesta a todos los problemas del organismo. Hay que considerar y analizar el significado temporal de las métricas.

El truco está en desarrollar métricas que sean simples y proporcionen información útil, a la vez que se corresponden con objetivos relacionados con la seguridad.

La tarea de las métricas de seguridad es contar o medir algo. Pero, ¿qué debería contarse? ¿Cómo puede medirse la seguridad? Muchos organismos cuentan los incidentes tratados, por ejemplo, virus detectados o eventos registrados. ¿Cómo

proporciona esto una medida de la calidad del programa de seguridad? ¿Cómo muestra esto el progreso?

Aunque ojo, los totales de incidentes son medidas poco fiables ya que el hecho de que se hayan registrado pocos incidentes no es reflejo fiel de que no hayan ocurrido.

La clave de las métricas de seguridad está en obtener medidas que tengan las siguientes características ideales:

- Deberían medir cosas significativas para el organismo.
- Deberían ser reproducibles.
- Deberían ser objetivas e imparciales.
- Deberían ser capaces de medir algún tipo de progresión a lo largo del tiempo.

En la práctica, casi todas las métricas de seguridad publicadas carecen una o varias de estas características. Se necesita un enfoque más sistemático para el desarrollo de métricas que encajen directamente en las características mencionadas anteriormente.

Ejemplos

Dominio	Indicador	Métrica
Gestión de activos	Grado de despliegue del inventario de activos.	Porcentaje de los activos de información analizados en cada fase (inventariados / identificados / responsables nominados / riesgos evaluados / clasificados).
Gestión de activos	Eficacia de los planes de tratamiento de riesgo.	Porcentaje de los activos de información crítica para los que se implementó los planes de tratamiento de riesgos de seguridad de la información y se mantuvo estos riesgos dentro de límites aceptables.

Control de acceso	Existencia y efectividad de controles de acceso a los sistemas operativos de las plataformas informáticas.	Nivel de existencia de registro seguro, ID de usuario único, técnicas de autenticación, contraseñas robustas, control de utilitarios del S.O., cierre de sesiones inactivas, etc. Y evaluación de estadísticas de vulnerabilidad y su seguimiento, si existiesen.
Gestión de incidentes	Grado de efectividad de la difusión acerca de los procedimientos de gestión de incidentes.	<p>Análisis estadístico de la cantidad y tipo de reportes, relativos a seguridad de la información</p> <p>De las estadísticas, crear y publicar un ranking de los centros de responsabilidad mostrando aquellos que son claramente conscientes de la seguridad frente a aquellos que no lo son.</p>

Acceder al documento “Indicadores SGSI” para profundizar en esta temática.