intiza

Norma de Gestión de Riesgos del SGSI

Versión: 3.0

NORMA DE GESTIÓN DE RIESGOS DEL SGSI	intiza
Tipo: Norma	Fecha vigencia: 21/11/2024
	Clasificación: Restringida
Código: NO-SI-04- Gestión de Riesgos del SGSI	Versión: 3.0

Contenido

1. Objetivo

Establecer los lineamientos para identificar y gestionar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información.

2. Alcance

El alcance está dado por todos los riesgos a los que están expuestos los activos de información, y activos de TI asociados a estos. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado debe ser identificado, analizado y evaluado.

3. Responsabilidades

Responsable del Área Involucrada participa en el análisis y evaluación de los riesgos definiendo la criticidad de los mismos y establece los planes de acción para mitigar dichos riesgos.

Seguridad de la Información es responsable de identificar y gestionar los riesgos manteniendo el control y la actualización de los mismos en el inventario de riesgos junto con el responsable del área involucrada en cada uno de ellos. Adicionalmente, es responsable de evaluar y documentar, con la aprobación del Comité de Seguridad, el nivel de riesgo (impacto y probabilidad).

Comité de Seguridad: es responsable de revisar y aprobar los planes de acción establecidos para mitigar los riesgos, como así también asumir aquellos riesgos que el negocio considere.

4. Desarrollo

En el desarrollo de la evaluación de los riesgos se deberá incluir un análisis de estos, como así también de la configuración de seguridad implementada en los Activos de TI y en la información de INTIZA, contemplando los estándares y buenas prácticas de seguridad del mercado.

Los resultados de la evaluación de riesgos deberán ser documentados y relacionados con el Inventario de Información y Activos de TI. Asimismo, estos resultados deberán ser considerados para las definiciones de medidas de protección a implementar, y para el desarrollo de otras tareas relativas a la administración de seguridad, como por ejemplo la respuesta ante incidentes, de forma tal de determinar niveles de urgencia y prioridad.

Cuando se planifiquen cambios significativos sobre los Activos de TI o cuando se produzcan cambios significativos a nivel del entorno y ambiente de negocio de INTIZA, se deberá efectuar una evaluación de la situación de riesgos resultante de forma tal de evaluar si las medidas de seguridad existentes deben ser revisadas y modificadas para que continúen siendo eficaces y apropiadas, manteniendo el nivel de riesgo aceptado por la Compañía.

4.1. Identificación del Riesgo

La situación de riesgos a los que están expuestos los Activos de información y la información de negocio de INTIZA deberá ser evaluada y revisada con frecuencia anual necesario, con el fin de garantizar que las prácticas de la organización reflejan adecuadamente la política y normas aplicadas, y que la situación de riesgo existente es razonable, tanto con lo definido y aceptado por la compañía, como con lo definido por las mejores prácticas en seguridad y gestión de riesgos.

Para la identificación de riesgos se debe:

Evaluar e identificar los riesgos a los que está expuesto un activo de acuerdo con los grupos de controles definidos en secciones propuestos por la Norma ISO 27002, ellos son:

- Controles organizacionales
- Controles de personas
- Controles físicos
- Controles tecnológicos

Se debe definir un enfoque o técnica para efectuar la identificación de riesgos, tales como checklists, brainstormings, cuestionarios, entrevistas, etc.

4.2. Análisis del Riesgo

Seguridad de la Información evaluará y documentará los riesgos a la que están expuestos los Activos de TI y la información de la Compañía, poniendo especial énfasis en aquellos Activos de TI e información críticos para el negocio.

El análisis de riesgos deberá realizarse siguiendo una metodología de gestión de riesgos donde se evalúen los mismos en función a su probabilidad de ocurrencia y su impacto en el negocio para establecer luego una ponderación del riesgo.

4.3. Evaluación de Riesgos

Se evaluarán los riesgos de los activos críticos de la compañía. Y deberán tratarse según la prioridad a tomar en cuenta:

- Afectación al negocio.
- El apetito de riesgo de la organización.
- Los requisitos de seguridad y de cumplimiento.
- El tipo y la severidad del riesgo sobre el activo.
- El coste de las distintas opciones de tratamiento.

Las decisiones que se tomen en este apartado deben basarse en el contexto interno y externo de la compañía, teniendo en cuenta los objetivos de la organización y el punto de vista de las partes interesadas.

4.4. Tratamiento de Riesgos

Luego de realizada la ponderación de los riesgos se deberá elaborar un plan de mitigación de estos. En la elaboración de dicho plan se deberá tener en cuenta la relación costo/beneficio del riesgo que se desea tratar, así como las consecuencias y las posibles acciones que se van a implementar.

La elaboración del plan de mitigación deberá realizarse en forma conjunta con el responsable del área involucrada y/o afectada por cada riesgo, estableciendo responsables y fijando fechas para su desarrollo.

Para todos los riesgos identificados se deberán establecer controles asociados que permitan disminuir la criticidad de los mismos y lograr un riesgo residual aceptable.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Metodología	Gestión de Riesgos de Seguridad de la Información	ME-SI-01
Registro	Matriz de Gestión de Riesgo del SGSI	RE-SI-05
Procedimiento	Gestión de Riesgos del SGSI	PR-SI-23

5.2. Definiciones

Término	Descripción
Riesgo residual	El riesgo residual es el riesgo que permanece después de se han hecho todos los esfuerzos para identificar y eliminar el riesgo (es decir, sus controles de mitigación).
Plan de mitigación	Se denomina Plan de Mitigación a las estrategias definidas por INTIZA que tratan de reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar.
Activos de TI	Los activos de TI (Tecnología de la Información. IT en inglés) son los recursos tecnológicos con los que toda empresa o entidad pública, cuenta para agilizar su gestión.
Brainstorming	La lluvia de ideas, también denominada tormenta de ideas, o "brainstorming", es una herramienta de trabajo grupal que facilita el surgimiento de nuevas ideas sobre un tema o problema determinado. La lluvia de ideas es una técnica de grupo para generar ideas originales en un ambiente relajado.

6. Historial de Versiones

NORMA DE GESTIÓN DE RIESGOS DEL SGSI	intiza
Tipo: Norma	Fecha vigencia: 21/11/2024
	Clasificación: Restringida
Código: NO-SI-04- Gestión de Riesgos del SGSI	Versión: 3.0

Versión	Fecha	Resumen de Cambios
1.0	01/07/2021	Creación de la norma de Análisis y Gestión de Riesgo.
1.0	28/10/2021	Aprobado por Comité de Dirección: MI-DI-01- Minuta del Comité de Dirección N° 1
2.0	01/10/2022	Cambio del nombre de la norma y ajustes en los lineamientos.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06 Minuta del Comité de Dirección N° 6.
3.0	21/11/2024	Se modificó el apartado “4.1. Identificación del Riesgo”, teniendo en cuenta la agrupación de los controles por secciones propuesta por la ISO 27002 de 2022 a cambio de los dominios que proponía la versión de 2013.
3.0	21/11/2024	Aprobado por Comité.