intiza

Metodología de Gestión de Riesgos de Seguridad de la Información

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO Consultoría Externa	 Carla Leiva - CISO	 Francisco Canale - Director

Contenido

1. Objetivo

Establecer e identificar 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

Este documento abarca todos los activos de información de INTIZA identificados y clasificados en el inventario de activos. 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.

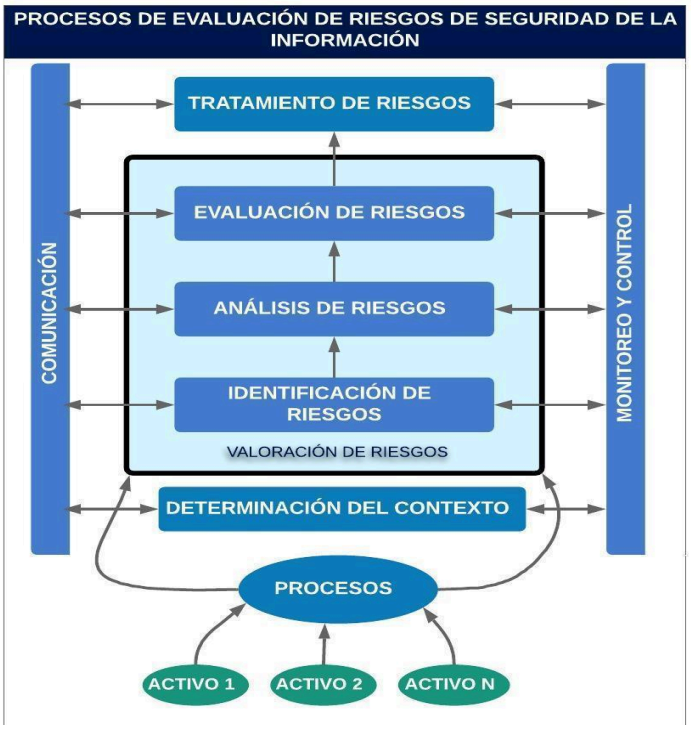
Seguridad de la información: Tendrá la responsabilidad de mantener el presente documento realizando las actualizaciones pertinentes respecto de modificaciones del marco regulatorio y/o procesos de la compañía.

4. Desarrollo

4.1. Metodología de Análisis de Riesgos

El proceso de evaluación de riesgos está diseñado para permitir a la organización identificar, analizar y evaluar sistemáticamente los riesgos de seguridad de la información asociados con un sistema o servicio de información junto con los controles necesarios para gestionarlos.

La metodología del análisis de riesgos tecnológicos se desarrolla de acuerdo con las siguientes definiciones y parámetros, para obtener un resultado objetivo que aporte al desarrollo del mejor plan de remediación acorde al negocio de INTIZA y su estructura, sin dejar de lado las consideraciones en la gestión de los servicios tecnológicos brindados por Tecnología. Los criterios de evaluación de Análisis de riesgos de TI se determinaron bajo los siguientes conceptos que determina su gestión:



4.2. Secciones y Controles

Para la realización del análisis de Riesgos de seguridad de la información se van a tener en cuenta las siguientes secciones y controles asociados de acuerdo con la ISO 27001 de 2022.

Sección	N.	Control
Controles Organizativos	5.1	Políticas de seguridad de la información
	5.2	Funciones y responsabilidades de la seguridad de la información
	5.3	Separación de funciones
	5.4	Responsabilidades de gestión

	5.5	Contacto con las autoridades
	5.6	Contacto con grupos de interés especial
	5.7	Inteligencia de Amenazas
	5.8	Seguridad de la información en la gestión de proyectos
	5.9	Inventario de información y otros activos asociados
	5.10	Uso aceptable de la información y otros activos asociados
	5.11	Devolución de activos
	5.12	Clasificación de la información
	5.3	Etiquetado de la información
	5.14	Transferencia de información
	5.15	Control de acceso
	5.16	Gestión de identidades
	5.17	Información de autenticación
	5.18	Derechos de acceso
	5.19	Seguridad de la información en las relaciones con los proveedores
	5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores
	5.21	Cadena de suministro de tecnología de la información y de las comunicaciones
	5.22	Seguimiento, revisión y gestión del cambio de los servicios con los proveedores
	5.23	Seguridad de la información para el uso de servicios en la nube
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
	5.25	Evaluación y decisión sobre eventos de seguridad de información
	5.26	Respuesta a incidentes de seguridad de la información

	5.27	Aprendizaje de los incidentes de seguridad de la información
	5.28	Obtención de pruebas
	5.29	Seguridad de la información durante la interrupción
	5.30	Preparación de las TIC para la continuidad delas actividades
	5.31	Identificación de requerimientos legales, estatutarios, regulatorios y contractuales
	5.32	Derechos de Propiedad Intelectual (DPI)
	5.33	Protección de los registros de la organización
	5.34	Protección y privacidad de la información de carácter personal
	5.35	Revisión independiente de la seguridad de la información
	5.36	Cumplimiento con políticas y estándares para la seguridad de la información
	5.37	Procedimientos operativos documentados
Controles de Personas	6.1	Investigación de antecedentes
	6.2	Términos y condiciones del empleo
	6.3	Concienciación, educación y capacitación en seguridad de la información
	6.4	Proceso disciplinario
	6.5	Responsabilidades ante la finalización o cambio
	6.6	Acuerdos de confidencialidad o no revelación
	6.7	Teletrabajo
	6.8	Reporte de eventos de seguridad de la información
Controles Físicos	7.1	Perímetro de seguridad física
	7.2	Controles de entrada física
	7.3	Seguridad de oficinas, despachos y recursos
	7.4	Supervisión de la seguridad física

	7.5	Protección contra las amenazas externas y ambientales
	7.6	El trabajo en áreas seguras
	7.7	Política de puesto de trabajo despejado y pantalla limpia
	7.8	Ubicación y protección de equipos
	7.9	Seguridad de los activos fuera de las instalaciones
	7.10	Medios de almacenamiento
	7.11	Apoyo a los servicios públicos
	7.12	Seguridad del cableado
	7.13	Mantenimiento de los equipos
	7.14	Reutilización o eliminación segura de equipos
Controles Tecnológicos	8.1	Dispositivos de punto final del usuario.
	8.2	Gestión de privilegios de acceso
	8.3	Restricción del acceso a la información
	8.4	Control de acceso al código fuente de los programas
	8.5	Autenticación segura
	8.6	Gestión de capacidades
	8.7	Controles contra malware
	8.8	Gestión de vulnerabilidades técnicas
	8.9	Gestión de la configuración
	8.10	Eliminación de la información
	8.11	Enmascaramiento de datos
	8.12	Prevención de la fuga de datos
	8.13	Copias de seguridad de la información
	8.14	Redundancia de las instalaciones de procesamiento de la información

	8.15	Registro
	8.16	Actividades de seguimiento
	8.17	Sincronización del reloj
	8.18	Uso de utilidades con privilegios del sistema
	8.19	Instalación de software en sistemas operativos
	8.20	Seguridad de redes
	8.21	Seguridad de los servicios de red
	8.22	Segregación de redes
	8.23	Filtrado web
	8.24	Uso de Criptografía
	8.25	Política de desarrollo seguro
	8.26	Requisitos de seguridad en aplicaciones
	8.27	Principios de ingeniería de sistemas seguros
	8.28	Codificación Segura
	8.29	Pruebas de seguridad en el desarrollo y aceptación
	8.30	Desarrollo subcontratado
	8.31	Separación de ambientes de desarrollo, prueba y producción
	8.32	Gestión del cambio
	8.33	Información de la prueba
	8.34	Controles de auditoría de sistemas de información

4.3. Determinación de contexto

Como vemos el proceso tiene como inicio la evaluación del contexto como punto de partida. Esto garantiza que los riesgos se toman a partir de las necesidades reales de las partes interesadas en relación a la Seguridad de la Información.

4.4. Análisis de riesgos

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

Para cada Activo de la información analizado, la evaluación de riesgos deberá establecer lo siguiente:

4.4.1. Probabilidad de ocurrencia

En esta etapa se debe definir la probabilidad de que una amenaza particular pueda explotar una vulnerabilidad y se produzca un evento que afecte el Activo de Información y por consiguiente ocurra un evento no deseado para el negocio. La Probabilidad puede ser clasificada como:

Probabilidad	Valor	Definición
Improbable	**1**	Solo podría ocurrir en casos excepcionales. Cada 5 años o más.
Incierto	**1,5**	No es muy probable que ocurra en la mayoría de las circunstancias. Una vez cada 3 años y medio.
Posible	**2**	Podría ocurrir en la mayoría de las circunstancias. Una vez cada 2 años y medio.
Probable	**2,5**	Probablemente ocurra en la mayoría de las circunstancias. Una vez cada año y medio.
Muy probable	**3**	Se espera que ocurra en la mayoría de las circunstancias. Una vez al año o más de una vez al año.

4.4.2. Análisis de impacto:

En esta etapa se debe identificar el impacto que sufrirá el negocio debido a la ocurrencia de un evento no deseado. Este paso identifica para cada activo el impacto cualitativo que ocasionaría la explotación de la vulnerabilidad. El Impacto puede ser clasificado como INSIGNIFICANTE, MENOR, MODERADO, MAYOR, CATASTRÓFICO.

Impacto	Valor	1. Legislaciones aplicables	2.Impacto organizacional	3. Impacto en el cliente	4. Efecto en organización	5.Confidencialidad	6. Integridad	7.Disponibilidad	8. Privacidad (Datos Personales
Insignificante	**1**	Ninguna	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
Menor	**1,5**	Normativa Interna	Operativo / Sector	Cliente interno (1 área)	Mínimo	Mínimo	Mínimo	Mínimo	Mínimo
Moderado	**2**	Contrato con Terceros	Táctico / Gerencial	Cliente interno (+1 área)	Moderado	Moderado	Moderado	Moderado	Moderado
Mayor	**2,5**	Regulación del sector	Estratégico /Compañía	Cliente externo (-50)	Atención	Grave	Grave	Grave	Grave
Catastrófico	**3**	Ley Nac, Prov o Municipal	Estratégico / Grupo	Cliente externo (+50)	Grave	Muy Grave	Muy Grave	Muy Grave	Muy Grave

4.4.3. Clasificación de riesgos:

La ponderación del riesgo consiste en establecer los niveles adecuados de calificación, tanto de la probabilidad como del impacto, para determinar realmente el nivel de vulnerabilidad en la Compañía ante situaciones previsibles. También se debe tener en cuenta los factores de riesgo enunciados durante el proceso de identificación.

Basados en todos los puntos anteriores se deberá definir para cada Activo de Información una matriz de riesgo en la cual se deberá ubicar para cada amenaza su valoración de riesgo definida, producto de la probabilidad de ocurrencia y el impacto asociado:

Clasificación del riesgo	Definición
Alto	Exige la atención del director / Gerente / CEO y directores generales.
Medio	Debe ser gestionado adecuadamente por directivos de nivel medio.
Bajo	Debe ser gestionado a nivel de Supervisor.

El cálculo del Riesgos se realizará con la siguiente fórmula:

Nivel = (Probabilidad * Impacto)

4.4.4. Mapa de calor de valoración de riesgos

Siendo los resultados posibles clasificados en la siguiente tabla:

CUADRO DE VALORACIÓN DE RIESGOS			1	1,5	2	2,5	3
			Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	3	Muy probable	3	4,5	6	7,5	9
	2,5	Probable	2,5	3,75	5	6,25	7,5
	2	Posible	2	3	4	5	6
	1,5	Incierto	1,5	2,25	3	3,75	4,5
	1	Improbable	1	1,5	2	2,5	3

4.5. Identificación de los Controles

Los controles se evalúan por su eficacia, es decir, para mitigar el riesgo tienen que estar implementados, funcionar correctamente y ser susceptibles de medición para analizar su eficiencia. Estos tipos de controles los clasificaremos de la siguiente manera:

4.5.1. Nivel de Control:

Describe el nivel de control necesario para mitigar los riesgos del proceso.

Nivel de control	Valor	Definición
Alto	3	El control implementado debe ser continuo y automatizado
Medio	2	El control implementado puede ser manual, pero debe ser calendarizado y constante
Bajo	1	El control implementado puede ser manual y ejecutarse en forma periódica

4.5.2. Estado de Nivel de Control:

Clasificaremos el estado del Nivel de Control actual en el proceso.

Estado de Nivel de Control aplicable	Definición
Sobrecontrol	El control excede en costo y esfuerzo al impacto del riesgo
Aceptable	El control es equilibrado en relación con el impacto del riesgo
Inaceptable	El control no cubre las necesidades de mitigación respecto del impacto del riesgo

4.5.3. Nivel de Recursos necesarios para el Control:

Clasificaremos el nivel de esfuerzo estimado para el control a realizar.

NIVEL DE RECURSOS DEL CONTROL	Definición	Nivel
DOCUMENTACIÓN	El control existe y se desarrolla informalmente. Debe ser documentado (Norma, procedimiento, registros)	**Bajo**
CAPACITACIÓN	El personal propio o de terceros debe ser capacitado en el control, la documentación no fue publicada y comunicada o el personal no sabe de su existencia	**Bajo**
IMPLEMENTACIÓN DEL CONTROL	El control no existe, y debe ser documentado, el personal capacitado e implementarse. No requiere automatizarse o adquirir una herramienta para su ejecución	**Medio**
AUTOMATIZACIÓN DEL CONTROL	El control no existe, y debe ser documentado, el personal capacitado e implementarse. Se requiere su automatización o adquirir una herramienta para su ejecución	**Mayor**

4.5.4. Capacidades del Control:

Establecemos las capacidades de control actual en el proceso.

CAPACIDADES DEL CONTROL	Valor	Definición
Inexistente	0%	No se aplican controles en lo absoluto - No existe
Inicial	20%	Los controles son iniciales y desorganizados – Inicial
Repetible	40%	Los controles siguen un patrón regular - Repetible
Definido	60%	Los controles se documentan y se comunican - Definido
Gestionado	80%	Los controles se monitorean y se miden - Administrado
Optimizado	100%	Las buenas prácticas se siguen y se automatizan – Optimizado

4.6. Determinación del Riesgo Residual

El Riesgo Residual surge a partir de la multiplicación de la Probabilidad inherente y el Impacto, luego lo dividimos por el nivel de control aplicable. Así, el Riesgo Residual es la pérdida potencial estimada del activo, luego de la aplicación de la efectividad de los controles.

Riesgo Residual = Nivel de Riesgo / Nivel de Control Aplicable

Clasificación del riesgo Residual	Valor
Alto	6-10
Medio	3-5
Bajo	1-2

4.7. Tratamiento de Riesgos

Luego de realizados los pasos metodológicos mencionados, se debe poner en conocimiento del resultado del análisis a la Dirección de INTIZA, detallando los activos con Riesgo que exceden nuestro apetito al riesgo, previendo para cada uno de ellos establecer el Plan de Acción a seguir, pudiendo ser uno de los siguientes:

TRATAMIENTO DE LOS RIESGOS						
Control de la Norma ISO/IEC 27001	**Plan de acción sugerido**	**Estado de tratamiento**	**Fecha Mitigación**	**Responsable del Tratamiento**	**Comentarios**	**TRATAMIENTO DEL RIESGO**

Tratamiento de riesgos	Definición
Elección de controles	Implementación y ejecución de controles
Transferencia a terceros	Contratación para la administración externa, contratación de seguros, contratación de servicios externos
Evitar el riesgo	Desconexión o apagado del activo que ocasiona el riesgo
Asumir el riesgo	Aceptación del riesgo

Adicionalmente la Dirección de INTIZA deberá revisar y aprobar el resultado del Análisis de Riesgos, así como los Planes de Acción a seguir para mitigar los riesgos identificados y que se proponen evitar, reducir o transferir.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Norma	Análisis y Gestión de Riesgos	NO-SI-04

5.2. Definiciones

Término	Descripción
Información	Se considera información a los diferentes conjuntos organizados de datos que utiliza la empresa.
Activo	Cualquier Recurso o Capacidad de IT. Los Activos de un Proveedor de Servicio de IT incluyen todo aquello que se pueda atribuir a la entrega del Servicio de IT.
Evento	Ocurrencia de un conjunto particular de circunstancias.
Frecuencia	Medición del número de ocurrencias de un evento por unidad de tiempo.
Probabilidad	Medida de la oportunidad de ocurrencia de un evento.
Riesgo	La oportunidad de que suceda algo que tendrá impacto en los objetivos definidos.
Consecuencia	Resultado o impacto de un evento.

Gestión del riesgo	Proceso sistemático para entender la naturaleza del riesgo y deducir el nivel del riesgo.
Control	Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.
Evaluación de controles	Revisión sistemática de los riesgos para garantizar que los controles aún son eficaces y adecuados.
Monitorear	Verificar, supervisar o medir regularmente el progreso de una actividad, acción o sistema para identificar los cambios en el nivel de desempeño requerido.
Mapa de calor	Un mapa de Calor también conocido como mapa de calor de riesgos, permite visualizar los valores de los riesgos identificados de manera gráfica que enfrenta la compañía. Ayuda a identificar y priorizar los riesgos asociados.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	21/12/2021	Creación de la Metodología de Gestión de Riesgos de Seguridad de la Información.
1.0	24/06/2022	Aprobado por Comité de Dirección: MI-DI-05 Minuta de Comité de Dirección N° 5.
2.0	21/11/2024	Adecuación de la metodología teniendo en cuenta los controles de la ISO 27001 de 2022, sección 4.2 *"Secciones y Controles".*

2.0	21/11/2024	Aprobado por CISO.
2.1	14/06/2025	Se incluyen los aspectos de seguridad de la información y privacidad para formalizar la evaluación de los mismos.
2.1	14/06/2025	Aprobado por CISO.