

FORMATO MAPA DE RIESGOS



Formato Mapa Riesgos

Proceso: Seguridad y privacidad de la información

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de los datos e información en la Entidad. Esto implica salvaguardar la información contra accesos no autorizados, modificaciones no deseadas, pérdidas accidentales o daños malintencionados. El proceso busca asegurar que la información esté disponible y accesible para aquellos usuarios autorizados que lo requieren, al mismo tiempo que se proteja contra amenazas y vulnerabilidades que podrían comprometer su seguridad.

Alcance: El alcance del proceso de seguridad y privacidad de la información abarca todas las medidas, políticas y procedimientos implementados para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de la Entidad. Esto incluye la protección contra accesos no autorizados, prevención de alteraciones no deseadas, garantía de un acceso adecuado y controlado a la información, así como la adopción de estrategias para hacer frente a posibles incidentes de seguridad, y mantener la conformidad con las regulaciones y normativas pertinentes. El proceso de seguridad y privacidad de la información se extiende a través de todas las dependencias de la Entidad, involucrando a los funcionarios, la tecnología, los procesos y la cultura organizacional, con el fin de mitigar riesgos y preservar la confianza y la integridad en la gestión de la información.

Fecha de revisión	18-25
Versión	3

Referencia	Identificación del riesgo				Análisis del riesgo inherente					Evaluación del riesgo - Valoración de los controles										Plan de Acción									
	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Atributos					Evaluación del riesgo - Nivel del riesgo residual					Plan de Acción	Responsable	Fecha Implementación	
																Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual Final	%	Impacto Residual Final	%				Zona de Riesgo Residual
1	Económico y Reputacional	Pérdida de integridad y disponibilidad de la información, generada por fallas en la actualización de políticas de seguridad y privacidad de la información	Software malicioso en plataformas tecnológicas. No contar con políticas de seguridad de la información. Amenazas tecnológicas o de ingeniería social que atentan a la integridad, seguridad y disponibilidad de la información.	Posibilidad de pérdida económica y/o reputacional como consecuencia de la afectación a la integridad, confidencialidad y/o disponibilidad de la información, generada por fallas en la actualización de políticas de seguridad y privacidad de la información, presencia de software malicioso, falta de actualizaciones en las plataformas tecnológicas y/o la aparición de amenazas tecnológicas emergentes.	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efectos publicitarios sostenibles a nivel país.	Catastrófica	100%	Extremo	1	El profesional de gestión del Área de TIC realiza la verificación de la implementación de soluciones de seguridad (antivirus y firewall) periódicamente y políticas de actualización regular conforme a lo validado y acordado con la Oficina de Seguridad y Privacidad de la información, a través de los controles correspondientes, con el fin de mitigar amenazas tecnológicas emergentes.	Probabilidad	Preventivo	Automático	50%	Documentación	Continua	Con Registro	Baja	30%	Catastrófica	Extremo	Reducir (mitigar)	1. Realizar una evaluación de los sistemas en busca de malware	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025
													2	El profesional de gestión del área TIC y/o los profesionales especializados del área TIC garantizan la actualización periódica de las plataformas tecnológicas conforme a las recomendaciones y/o actualizaciones lanzadas por el fabricante y las políticas establecidas en el manual de seguridad de la información.	Probabilidad	Preventivo	Manual	40%	Documentación	Continua	Con Registro	Muy Baja	18%	Catastrófica	Extremo	Reducir (mitigar)	Realizar seguimiento a las actualizaciones periódicas en las plataformas tecnológicas conforme a lo establecido en las políticas establecidas en el manual de seguridad de la información	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025
2	Económico y Reputacional	Pérdida de confidencialidad y/o disponibilidad de la información, generada por acceso no autorizado a datos de información	Políticas de contraseñas débiles. Falta de apropiación de las políticas de contraseñas por parte de los funcionarios. Personal interno malicioso. Falta en la implementación de controles de acceso a los sistemas de información. Errores en la implementación de novedades de personal en los sistemas de información. Falta en los controles de acceso a las sedes de trabajo. Desatención por parte de los funcionarios de las políticas de controles de acceso y/o seguridad física. No contar con matrices de roles y perfiles. Uso de credenciales de acceso a recursos tecnológicos que han sido asignadas a otros usuarios.	Posibilidad de pérdida económica y/o reputacional por la pérdida de integridad, confidencialidad y/o disponibilidad debido al acceso no autorizado a la información, derivado de debilidades en los controles de acceso físicos y lógicos, fallas en la gestión de credenciales, y el incumplimiento de las políticas de seguridad por parte de los funcionarios.	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efectos publicitarios sostenibles a nivel país.	Catastrófica	100%	Extremo	1	El profesional de gestión de la Oficina de Seguridad y Privacidad de la Información establece políticas de contraseñas robustas y autenticación de dos factores en los sistemas de información que se puedan implementar.	Probabilidad	Preventivo	Manual	40%	Documentación	Continua	Con Registro	Baja	30%	Catastrófica	Extremo	Reducir (mitigar)	1. Revisar y fortalecer las políticas de contraseñas	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025
													2	El profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones garantiza la implementación de políticas de contraseñas robustas y autenticación de dos factores en aquellos sistemas de información que se puedan implementar para garantizar las políticas de control de acceso.	Probabilidad	Preventivo	Automático	50%	Documentación	Continua	Con Registro	Muy Baja	18%	Catastrófica	Extremo	Reducir (mitigar)	2. Implementar la autenticación de dos factores en los sistemas de información que no generen incompatibilidad técnica	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025
													3	Todos los funcionarios atienden y aplican las políticas de contraseñas establecidas en el manual de seguridad de la información.	Probabilidad	Preventivo	Automático	50%	Documentación	Continua	Con Registro	Muy Baja	5%	Catastrófica	Extremo	Reducir (mitigar)	3. Capacitar y sensibilizar al personal en buenas prácticas de seguridad	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025
													4	Los profesionales especializados del Área TIC, y el Profesional de gestión del Área TIC, de manera mensual, revisan la matriz de roles y perfiles de los sistemas de información para validación de los administradores lógicos y garantizar su implementación en los sistemas de información, con el fin de garantizar el acceso restringido a la información conforme a las funciones.	Probabilidad	Preventivo	Manual	40%	Documentación	Continua	Con Registro	Muy Baja	5%	Catastrófica	Extremo	Reducir (mitigar)	2. Implementar sistemas de monitoreo de actividad de usuarios con alertas por comportamiento sospechoso	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2025

