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 requieran, al mismo tiempo que se protege 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	nov-23
Versión:	1

Identificación del riesgo							Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual							Plan de Acción		
																Atributos															
Referencia	Impacto	Causa Inmediata	Causa Raiz	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	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación
1	Económico y Reputacional	Pérdida de integridad, confidencialidad y/o disponibilidad de la información	Software malicioso en sistemas de información. No contar con actualizaciones de las plataformas tecnológicas.	Posibilidad de pérdida económica y/o reputacional por la pérdida de integridad, confidencialidad y/o disponibilidad de la información, generada por un software malicioso en los sistemas de información, y/o por no contar con las debidas actualizaciones en las plataformas tecnológicas de la entidad	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	La Oficina de Seguridad y Privacidad de la Información y/o Área de TIC implementan soluciones de seguridad (antivirus y firewalls) y políticas de actualización regular.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30,0%	Baja	30%	Catastrófico	100%	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	31/12/2023
																													2. Implementar soluciones de seguridad en todos los sistemas	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													3. Establecer un plan de actualizaciones mensuales	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
2	Económico y Reputacional	Materialización de un acceso no autorizado a datos sensibles	Débiles políticas de contraseñas	Posibilidad de pérdida económica y/o reputacional por la materialización de un acceso no autorizado a datos sensibles, debido a débiles políticas de contraseñas	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	La Oficina de Seguridad y Privacidad de la Información y las Comunicaciones implementan políticas de contraseñas robustas y autenticación de dos factores.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Baja	36%	Catastrófico	100%	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	31/12/2023
													2	El Área de Tecnologías de la Información y las Comunicaciones implementan políticas de contraseñas robustas y autenticación de dos factores.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	18,0%	Muy Baja	18%	Catastrófico	100%	Extremo	Reducir (mitigar)	2. Implementar la autenticación de dos factores en todos los sistemas	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													3. Capacitar 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	31/12/2023
3	Económico y Reputacional	Pérdida o alteración permanente de datos críticos	Falta de copias de respaldo o protección de integridad de datos	Posibilidad de pérdida económica y/o reputacional por la pérdida o alteración permanente de datos críticos debido a Falta de copias de respaldo o protección de integridad de datos	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	La Oficina de Seguridad y Privacidad de la Información, y Área de TIC establecen rutinas regulares de copias de seguridad	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30,0%	Baja	30%	Catastrófico	100%	Extremo	Reducir (mitigar)	1. Identificar los datos críticos que necesitan respaldo	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													2. Implementar un sistema automatizado de copias de seguridad	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													3. Probar regularmente la restauración de datos a partir de las copias de respaldo	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023

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 requieran, al mismo tiempo que se protege 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	nov-23
Versión:	1

Identificación del riesgo							Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual							Plan de Acción		
																Atributos															
Referencia	Impacto	Causa Inmediata	Causa Raiz	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	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación
4	Económico y Reputacional	Fuga de información (divulgación no autorizada de información confidencial)	Personal interno malicioso	Posibilidad de pérdida económica y/o reputacional por divulgación no autorizada de información confidencial debido a personal interno malicioso	Fraude Interno	365	Media	60%	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor	80%	Alto	1	La Oficina de Seguridad y Privacidad de la Información, y el Área de TIC implementan controles de acceso basados en roles y monitoreo de actividades del personal.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Baja	36%	Mayor	80%	Alto	Reducir (mitigar)	1. Revisar y actualizar los roles y permisos de acceso	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información y Profesional de Gestión Área TIC	31/12/2023
																													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	31/12/2023
																													3. Realizar verificaciones de antecedentes en el proceso de vinculación	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información y Profesional de Gestión Área TIC	31/12/2023
5	Económico y Reputacional	Interrupción de servicio críticos	Fallas en el ecosistema tecnológico de la entidad	Posibilidad de pérdida económica y/o reputacional por interrupción de servicios críticos, debido a fallas en el ecosistema tecnológico de la entidad	Fallas Tecnologicas	365	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	La Oficina de Seguridad y Privacidad de la Información, y el Área de TIC implementan sistemas de redundancia y planes de continuidad del negocio	Probabilidad	Detectivo	Automático	40%	Documentado	Continua	Con Registro	36,0%	Baja	36%	Moderado	60%	Moderado	Reducir (mitigar)	1. Identificar los sistemas y servicios críticos	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													2. Implementar soluciones de redundancia donde sea necesario	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
																													3. Elaborar y poner a prueba un plan de continuidad del negocio	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023
6	Económico y Reputacional	Pérdida de integridad, confidencialidad y/o disponibilidad de la información	Desconocimiento en seguridad por parte del usuario. Falencias en la capacitación de seguridad	Posibilidad de pérdida económica y/o reputacional por pérdida de integridad, confidencialidad y/o disponibilidad de la información, debido a la falta de conciencia y comprensión de los principios básicos de seguridad de la información por parte de los usuarios.	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	La Oficina de Seguridad y Privacidad de la Información realiza capacitaciones en el marco del plan de capacitaciones de la entidad, con respecto a seguridad y privacidad de la información, enfocado a los funcionarios.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Baja	36%	Moderado	60%	Moderado	Reducir (mitigar)	1. Realizar capacitaciones periódicas de seguridad de la información a los funcionarios de la entidad y realizar capacitaciones de refuerzo a los funcionarios reincidentes	Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y Profesional de Gestión Área TIC	31/12/2023

Fuente: Adaptado de Curso Riesgo Operativo Universidad del Rosario por Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

CONTROL DE CAMBIOS

VERSIÓN Y FECHA	DESCRIPCIÓN
Versión 1 Noviembre de 2023	Nueva matriz para el proceso de seguridad de la información.

ELABORADO POR:

ALVARO IVAN TORRES GONZALEZ

Firmado digitalmente por ALVARO IVAN TORRES GONZALEZ
Fecha: 2023.11.09 08:41:59 -05'00'

ÁLVARO IVÁN TORRES GONZÁLEZ
Profesional de gestion de la Oficina de Seguridad y Privacidad de la Información

APROBADO POR:

RUBEN DARIO OCHOA ARBELAEZ

Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ

RUBÉN DARÍO OCHOA ARBELÁEZ
Director General