

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EPUXUA AVANZA

CONTENIDO

1.	INTRODUCCIÓN	3
2.	DEFINICIONES.....	3
3.	OBJETIVOS.....	4
3.1.	GENERAL.....	4
3.2.	OBJETIVOS ESPECIFICOS	4
4.	ALCANCE.....	4
5.	DOCUMENTOS RELACIONADOS.....	5
6.	METODOLOGÍA DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	5
7.	DESARROLLO DE LA METODOLOGÍA.....	6
7.1.	IDENTIFICACIÓN DE RIESGOS	6
7.2.	VALORACIÓN DE LOS RIESGOS.....	6
7.2.1.	Identificación de las Vulnerabilidades.....	8
7.3.	ANÁLISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.....	10
7.3.1.	Evaluación Del Riesgo.....	10
7.4.	EVALUACIÓN DE LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS.....	11
8.	PLAN DE IMPLEMENTACIÓN.....	13
9.	RECURSOS.....	16

1. INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es importante que dentro de las organizaciones el plan de tratamiento de riesgos de Seguridad y Privacidad de la información este orientado estratégicamente al desarrollo de una cultura de carácter preventivo, donde cada usuario entienda los riesgos y las afectaciones que se puede presentar permitiendo tomar medidas que disminuyan la materialización de estos.

Para el tratamiento de riesgos de debe contar con un plan de gestión de riesgos para garantizar la continuidad del negocio, planeando acciones que disminuyan la afectación de los procesos, Por este motivo, se ha visto la necesidad de desarrollar la identificación, análisis, tratamiento, evolución y monitoreo de riesgo de seguridad de la información.

2. DEFINICIONES

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Aceptación de riesgo: Decisión de asumir un riesgo

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados

Control: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad

Dueño del riesgo sobre el activo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

3. OBJETIVOS

3.1. GENERAL

Definir las acciones necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, definiendo los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza, así como permitir la recuperación del sistema.

3.2. OBJETIVOS ESPECIFICOS

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, acorde a las necesidades de la entidad.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Dar a conocer la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Definir los principales elementos a proteger en la entidad.
- Identificar las principales amenazas en la entidad.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

4. ALCANCE

Proporcionar una metodología para realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, que permita sostener los procesos de la entidad, y prevenir incidentes que puedan afectar el logro de los objetivos, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

5. DOCUMENTOS RELACIONADOS

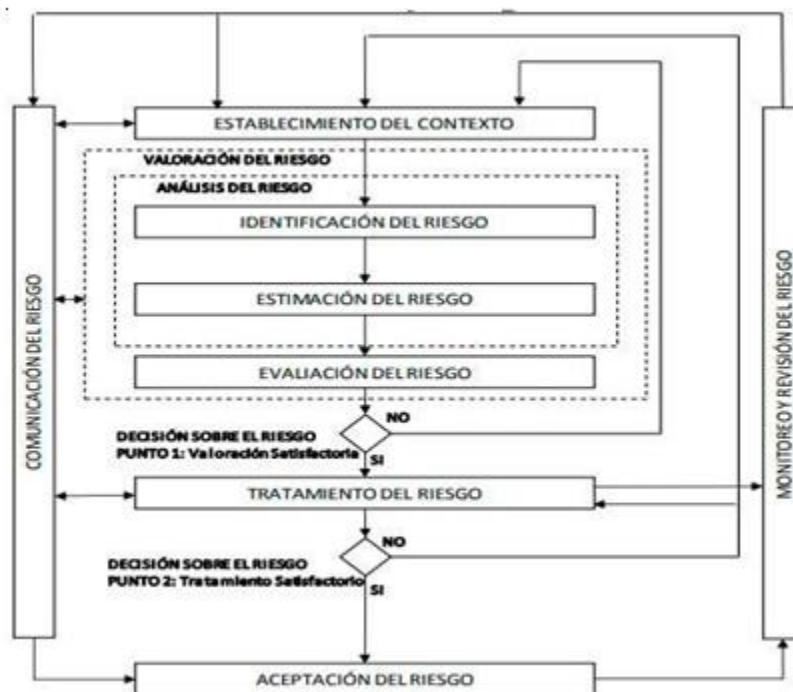
- Política General de Seguridad y Privacidad de la Información.
- Manual de Políticas de Seguridad y Privacidad de la Información.
- Norma ISO 31000:2009.
- Inventario de activos de información.

6. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se implementará una metodología de Gestión de Riesgos de Seguridad de la Información basada en la norma ISO 31000 y en la guía de Gestión del Riesgo Seguridad y Privacidad de la Información de MinTic, como se ilustra a continuación.



Proceso Gestión del Riesgo ISO 31000



Proceso para la administración del riesgo en seguridad de la información NTC-ISO/IEC 27005

7. DESARROLLO DE LA METODOLOGÍA

A continuación, se detallan las distintas etapas de la metodología de gestión de riesgos:

7.1. IDENTIFICACIÓN DE RIESGOS

En esta etapa los encargados de Riesgos buscarán identificar los principales riesgos críticos a los que está expuesta la entidad, en los activos de información y que pudieran afectar el cumplimiento de los objetivos y/o estrategias definidas, la identificación puede ser a través de reuniones, encuestas, bases de datos o matrices de riesgo de ejercicios previos.

Una vez identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo estratégico, imagen, financieros, operacional, tecnológicos y cumplimiento.

7.2. VALORACIÓN DE LOS RIESGOS

En este paso se genera una lista completa de los riesgos de cada uno de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los objetivos de la Entidad, los cuales podrán ser identificados y evaluados teniendo en cuenta los criterios de evaluación definidos. En este

proceso se debe realizar las siguientes actividades:

- Identificar el flujo de información de cada uno de los procesos
- Identificar las vulnerabilidades que existen en el proceso.
- Identificar las amenazas que podrían materializarse dadas las vulnerabilidades existentes.
- Definir las escalas a utilizar

De acuerdo con los lineamientos para la gestión de riesgos digital en entidades públicas emitida por el DAFP, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados, a continuación, se describen una serie de amenazas comunes.

Deliberadas (D), fortuito (F) o ambientales (A).

Tipo	Amenaza	Origen
Daño físico	Fuego	A, D, F
	Agua	A, D, F
	Polvo, corrosión, congelamiento	A, D, F
Eventos naturales	Fenómenos climáticos	F
	Fenómenos sísmicos	F
	Fenómenos meteorológicos	F
	Inundaciones	F
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D, F
	Falla en equipo de telecomunicaciones	A, D, F
	Perdida de suministro de energía	A, D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Hurto de medios o documentos	D
	Recuperación de medios reciclados o desechados	D
	Datos provenientes de fuentes no confiables	D
	Manipulación con hardware	D
	Manipulación con software	D

Tipo	Amenaza	Origen
	Divulgación	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
	Uso de software falso o copiado	D, F
	Corrupción de los datos	D, F
Compromiso de las funciones	Error en el uso	D, F
	abuso de derechos	D
	Falsificación de derechos	D
Amenazas humanas	Pirata informático, intruso ilegal	D
	Criminal de la computación	D
	Terrorismo: Chantaje Destrucción	D
	Explotación Venganza, Ganancia política	
	Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	D

7.2.1. Identificación de las Vulnerabilidades.

Se deben identificar vulnerabilidades (debilidades) de acuerdo con los siguientes tipos:

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de terminación de sesión cuando se abandona la estación de

Tipo	Vulnerabilidad
Software	trabajo.
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Gestión deficiente de las contraseñas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
	Arquitectura insegura de la red
	Gestión inadecuada de la red
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
	Uso incorrecto de software y hardware
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio y los recintos
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de mecanismos de monitoreo para brechas en la seguridad

Tipo	Vulnerabilidad
	Ausencia de procedimiento formal para la documentación del MSPI.
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de política sobre limpieza de escritorio y pantalla
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad

7.3. ANÁLISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Estos criterios de riesgo estarán revisándose de forma permanente, dado los cambios que pueden ocurrir en la organización.

Al definir los criterios de riesgo, se tendrán en cuenta:

- La naturaleza, los tipos de causas y consecuencias que pueden ocurrir y como se van a medir.
- La manera de definir la probabilidad de ocurrencia de un evento.
- La forma de determinar el nivel de riesgo.
- Niveles de riesgo aceptable para la organización.

De esta forma se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

7.3.1. Evaluación Del Riesgo

De acuerdo a la guía de gestión del riesgo, seguridad y privacidad de la información, se utilizará la “Matriz de Calificación, Evaluación y Respuesta a los Riesgos”, obteniendo la forma de calificar los riesgos con los niveles de impacto y probabilidad.

“Matriz de Calificación, Evaluación y respuesta a los Riesgos”

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

7.4. EVALUACIÓN DE LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS

En la evaluación de los controles se tendrá en cuenta los criterios de cada uno de los riesgos identificados, iniciando por la evaluación los controles ya establecidos de la entidad determinado la efectividad frente al riesgo, de ser necesario se reevaluará y se determinará nuevo control, en este punto se utilizará la tabla de “estructura de nuevos controles” que presenta la guía de controles de MSPI.

Tabla Estructura de controles

Política general			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
	...		

Fuente: Guía – Controles del MSPI

Igualmente se utilizará las “Tablas para valoración de controles” que entrega la guía para la cuantificación de los controles.

PÁRAMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de la ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Tablas para valoración de controles- DAFP

8. PLAN DE IMPLEMENTACIÓN

Mapa de riesgos

Identificación del Riesgo						Valoración del Riesgo de corrupción						
PROCESO	Tipo Proc	OBJETIVO	Evento	Causa	Impacto	Análisis del Riesgo			Controles		PROGRAMACIÓN DE ACCIONES	
						PROBABILIDAD	IMPACTO	ZONA DEL RIESGO ABSOLUTA	NOMBRE	RESPONSABLE	Fecha de inicio	Fecha terminación
GESTION DE LA INFORMACIÓN	Apoyo	Diseñar e implementar estrategias de comunicación de las actividades que realiza la Entidad a nivel interno y externo.	Divulgación de información no veraz sobre los productos y servicios, gestión o actividades de EPUXUA AVANZA con el fin de obtener un beneficio particular en detrimento de los recursos y/o activos de la Entidad	Manejo intencional de la información para favorecer intereses particulares	Imagen / Reputación Operacional	Rara vez	Mayor	Baja	Verificación previa de la información y validación por parte del Subgerente que se requiera	Subgerente Administrativo y Financiero Subgerente Técnico Asesor Jurídico	1/02/2021	31/12/2021
		Identificar, evaluar controlar y definir acciones para mitigar riesgos que afecten el cumplimiento del objeto de la Entidad.	Pérdida de la información en medio digital, almacenada en los servidores de la entidad o por medio de los servicios tecnológicos disponibles, debido a la alteración o	Acción intencional de un colaborador de la Entidad.	operacional /reputación	Rara vez	Catastrófico	Moderada	Capacitación sobre seguridad informática a los usuarios	Subgerente de Gestión Administrativo y Financiero y de Gestión Humana		

		modificación con el fin de obtener un beneficio particular			Rara vez	Catastrófico	Moderada	Software y hardware de protección de información (Firewall, DNS, de página web, antivirus)		
					Rara vez	Catastrófico	Moderada	Definición de derechos de acceso (perfil de autorización) de usuarios a los sistemas de información y Backup institucional.		
	Planificar, liderar y controlar las estrategias de gestión, uso y apropiación de las tecnologías de la información y las comunicaciones.	Impacto operacional debido a que se afecta el funcionamiento de la plataforma Tecnológica de EPUXUA AVANZA con el fin de obtener un beneficio particular en detrimento de los recursos y/o activos de la Entidad por causa de la acción intencional de	Acción intencional de funcionarios y terceros	operacional	Rara vez	Catastrófico	Moderada	Segregación de roles y funciones en el área de Tecnología de Información. Gestión de usuarios Control de acceso a la red de datos por personas externas Seguimiento a los servicios de tecnología contratados con terceros	Subgerente de Gestión Administrativo y de Gestión Humana	

			Pérdida y/o divulgación de información confidencial por parte de funcionarios y terceros, relacionada con la Entidad, con el fin de obtener un beneficio particular en detrimento de los recursos y/o activos de la Entidad	Acción intencional de colaboradores y terceros de la Entidad mediante el acceso no autorizado.	Imagen / Reputación	Rara vez	Catastrófico	Moderada	Gestión de usuarios	Subgerente de Gestión Administrativo y Financiero y de Gestión Humana
									Acuerdos de confidencialidad de la información	
									Capacitación sobre seguridad informática a los usuarios	
									Desactivar los usuarios que no laboran en la identidad mediante comunicación interna	

9. RECURSOS

Para gestión de riesgos de Seguridad y Privacidad de la Información, La Empresa Pública del Municipio de Soacha, EPUXUA AVANZA E.I.C.E. cuenta con:

RECURSOS	VARIABLE
Humanos	Personal en capacitación para la gestión del riesgo de seguridad digital. El área de tecnologías TIC, es responsable de las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo del Departamento Administrativo de la Función Pública (DAFP). Guía de gestión del riesgo - Seguridad y Privacidad de la Información - MinTic Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Aspectos de mejora continua, monitoreo y auditorías. Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquirir con oportunidad y calidad técnica los bienes y servicios requeridos; recursos humanos, técnicos.

Aprobó: Comité Institucional de Planeación y Gestión- MIPG
Revisó: Mercedes Rodríguez González -Subgerente de Gestión Administrativa, Financiera y de Gestión Humana
Elaboró Jimmy Julian Vallejo Caro -Profesional Universitario