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

GERMÁN DARÍO RODRÍGUEZ PARRA
Gerente

2022

Tabla de Contenido

.

1 INTRODUCCIÓN 3

2 OBJETIVOS 3

3 ALCANCE 3

4 VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN 4

5 IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD DIGITAL 5

6 CONTROL DE CAMBIOS 9

7 ELABORO, REVISO Y APROBÓ 10

1 INTRODUCCIÓN

El Instituto Financiero para el Desarrollo del Huila INFIHUILA, ha establecido políticas de Seguridad de la Información y Ciberseguridad, temiendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soportará el habilitador transversal de la Seguridad de la Información del Infihuila; dentro de los instrumentos que apoyan la implementación del MSPI de la Entidad, en la Fase 3 – Implementación, se encuentra la necesidad de definir el Plan de Tratamiento de Riesgos de Información que permitirá la identificación, análisis, valoración y tratamiento de riesgos relacionados con la información institucional ya sea física o digital, en cada uno de sus procesos, con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad.

2 OBJETIVOS

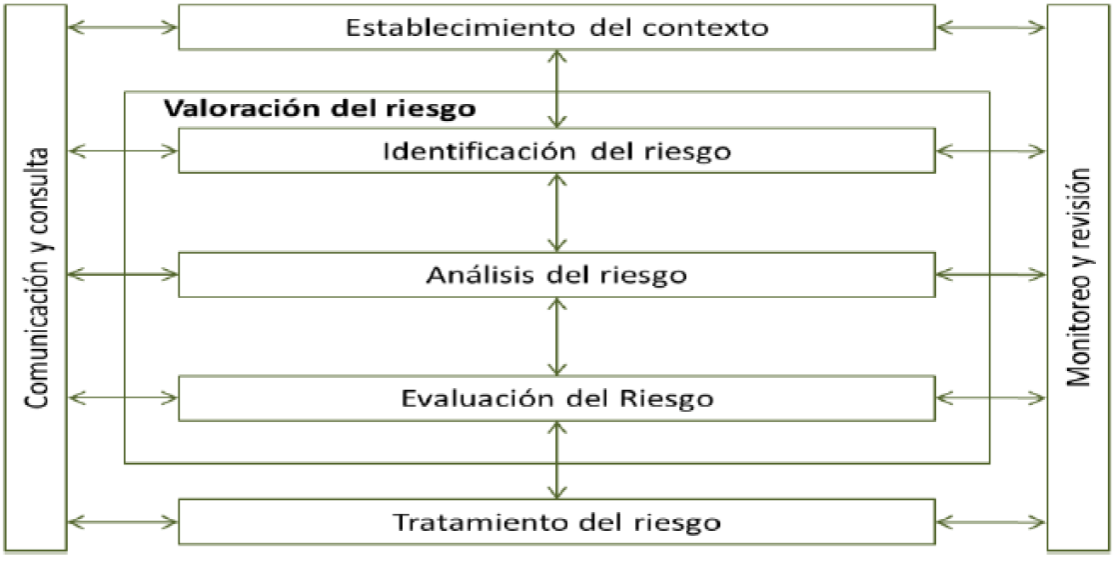
Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica, que permita a los responsables de los procesos del Infihuila gestionar los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información, que hacen parte del Registro de Activos de Información del Infihuila (RAI) y que sean identificados con una criticidad alta por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad.

3 ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información del Infihuila identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información del Infihuila (RAI); con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4 VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Se tomará como base para la gestión de los riesgos de información, el ejercicio documentado de identificación del contexto organizacional, aplicado a cada uno de los procesos estratégico, misional y de apoyo de la entidad; de igual forma se parte de la metodología de tratamiento de riesgo de la Entidad, definido en el Manual del Sistema Administración del Riesgo Operativo - SARO, razón por la cual este documento solamente abordará las etapas de identificación y clasificación del riesgo cuando se trata de un "Riesgo de Seguridad Digital".



Fuente: Norma ISO 31000 versión 2018.

5 IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD DIGITAL

Este documento apoya al dueño de la información o delegado para la etapa de identificación y clasificación del riesgo cuando se trata de un "Riesgo Seguridad Digital", alineado con el Manual del Sistema Administración del Riesgo Operativo - SARO, en donde es necesario tener en cuenta que estos riesgos serán tratados en sus etapas iniciales y finales de acuerdo al mencionado manual y para los activos de información que en el Registro de Activos de Información de la SDP (RAI) hayan sido clasificados como de criticidad "Alta" por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad, razón por la cual se consideraría que existe un riesgo de la información en alguno de éstos tres pilares.

Al respecto, se debe tener en cuenta que la criticidad de los activos de información fue valorada de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de Min TIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital, midiéndose por los tres pilares de la seguridad de la información "CONFIDENCIALIDAD", "INTEGRIDAD", "DISPONIBILIDAD" según la clasificación que determina el numeral 7 de dicha Guía, de la siguiente manera:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tras la valoración del activo de información por cada uno de los tres pilares, se clasifica el Activo en el nivel de criticidad "ALTA", "MEDIA" ó "BAJA"), de acuerdo con las condiciones de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC de la siguiente manera:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

El resultado de esta valoración se refleja finalmente en el documento Registro de Activos de Información (RAI), a partir del cual se seleccionan para tratamiento de riesgos, todos los activos de información clasificados con nivel de criticidad "ALTA"

De acuerdo con lo especificado en la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas, se deberá especificar la amenaza de acuerdo a la siguiente tabla de referencia:

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Tras el registro de una amenaza, se deberán especificar las vulnerabilidades, de acuerdo con la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas, se deberá especificar la vulnerabilidad de acuerdo con la siguiente tabla de referencia:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
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
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso

Tipo	Vulnerabilidades
	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 mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

6 PLAN DE IMPLEMENTACIÓN

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLES
ACTIVOS DE IMPLEMENTACIÓN	Matriz de riesgos identificados	Creación de la de Matriz de riesgos identificados de seguridad digital, de acuerdo con el resultado obtenido en el levantamiento del Registro de Activos de Información (RAI) y de los riegos identificada para cada uno de los activos de información	Grupo de trabajo Gestión TICS
ACTIVIDADES DE REPORTE	Listado de activos críticos y listado de	Identificar si un activo es considerada infraestructura crítica, si su impacto o afectación podría superar el IMPACTO SOCIAL, IMPACTO ECONÓMICO y EL IMPACTO AMBIENTAL	Grupo de trabajo Gestión TICS
ACTIVIDADES DE CONTROL	Monitoreo y Revisión	Generación, presentación y reporte de Actividades	Control Interno
	Seguimiento	Realiza el seguimiento	Planeación

7 CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
Enero 2020	1	Elaboración del Plan
Enero 2021	2	Actualización
Enero 2022	3	Actualización

8 ELABORO, REVISO Y APROBÓ

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Gestión TIC	**NOMBRE:** Idelber Pabón López	**NOMBRE.** Comité Gestión TI Acta 001 -2022
CARGO: Profesionales de apoyo	**CARGO:** Profesional Universitario	**CARGO:** Comité Tic
FECHA: 27/01/2022	FECHA: 27/01/2022	FECHA: 27/01/2022