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

ALCALDIA DE GIRARDOT

VIGENCIA 2023

Tabla de contenido

INTRODUCCIÓN

La gestión de los riesgos de Seguridad de la información se desarrolla con el fin de reducir la pérdida y brindar protección a la información en los diferentes procesos, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que la entidad cuente con un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad aplicado a la Alcaldia Municipal de Girardot.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información.

Objetivo General

Elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información, alineado a la metodología de riesgos del DAFP, para mitigar la pérdida de activos de información en la Alcaldía Municipal de Girardot.

Objetivos Específicos

- Identificar los activos de información a través del inventario del mismo.
- Establecer los controles de la seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de la información.
- Identificar las principales amenazas que afectan a los activos de información.
- Definir soluciones para minimizar los riesgos a los que están expuestos cada activo de información.
- Evaluar y comparar el nivel de riesgo actual con el generado después de implementado el plan de tratamiento de riesgos de seguridad y privacidad de la información.

Marco Normativo y Definiciones

Norma ISO 27005	Tecnología de la información, Técnicas de seguridad, Gestión de riesgo en la seguridad de la información.
Normal ISO 27001	Especificaciones para un Sistemas de gestión de Seguridad de información.
Norma ISO 27002	Código de buenas prácticas en el Sistema de gestión de Seguridad de la Información.
Ley 1712 de 2014	**Acceso a la Información Pública** - Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados
Norma ISO 27000	**Activo** - En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, información, etc) que tenga valor para la organización.
Ley 594 de 2000	**Archivo** - Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o

	institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.
Norma ISO 27000	**Amenazas** - Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización
Norma ISO 27000	**Análisis de Riesgo** - Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Norma ISO 27000	**Auditoría** - Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.
Ley 1581 de 2012	**Bases de Datos Personales** - Conjunto organizado de datos personales que sea objeto de Tratamiento
CONPES 3701	**Ciberseguridad** - Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
Resolución CRC 2258 de 2009	**Ciberespacio** - Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.
	Control - Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Ley 1712 de 2014	**Datos Abiertos** - Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos
Ley 1581 de 2012	**Datos Personales** - Cualquier información

	vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Decreto 1377 de 2013	**Datos Personales Públicos** - Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
Ley 1581 de 2012	**Datos Personales Privados** - Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular
	Datos Personales Mixtos - Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
Decreto 1377 de 2013	**Datos Personales Sensibles** - Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
Norma ISO 27000	**Gestión de incidentes de seguridad de la información** - Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Norma ISO 27000	**Plan de continuidad del negocio** - Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro
Norma ISO 27000	**Plan de tratamiento de riesgos** - Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles

	necesarios para proteger la misma.
Norma ISO 27000	**Riesgo** - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Norma ISO 27000	**Sistema de Gestión de Seguridad de la Información SGSI** - Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Alcance

Crear la línea base del tratamiento de riesgos en la alcaldía municipal de Girardot, facilitando la identificación de los riesgos que se encuentran presentes en la entidad; de la misma manera los funcionarios conozca el proceso de mitigación de riesgos para lograr minimizar la pérdida de información o daños en los equipos.

Visión General para Administración del Riesgo de Seguridad de la Información

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo:

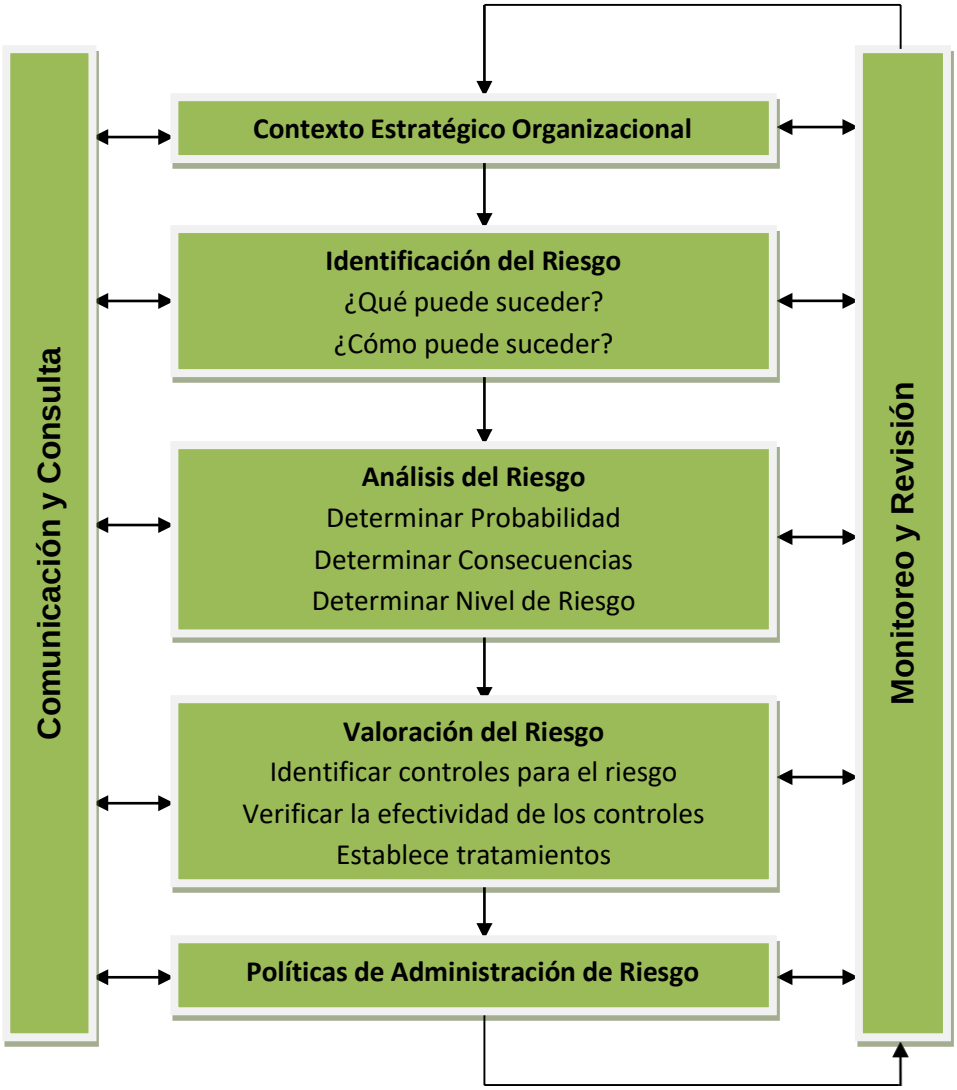

Imagen 1. Tomado de la Cartilla de Administración de Riesgos del DAFP

- Proceso para la administración del riesgo en seguridad de la información:

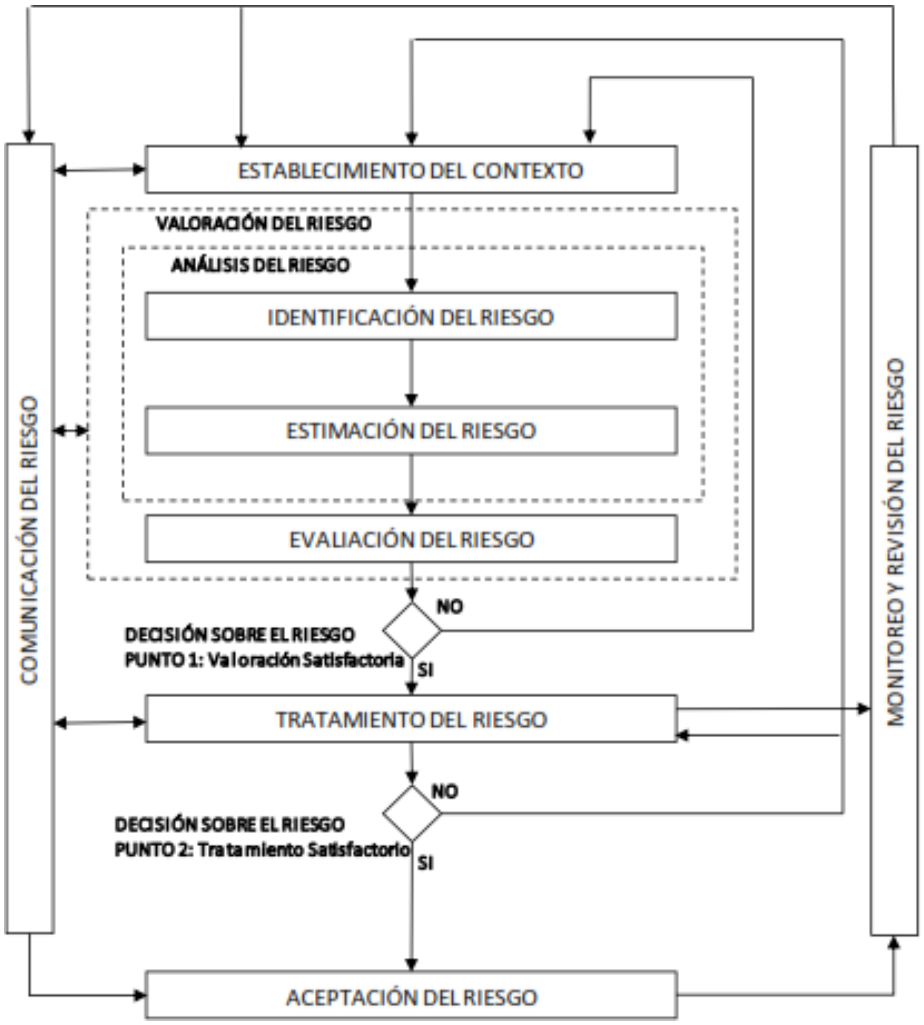

Imagen 2. Tomado de la NTC-ISO/IEC 27005

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevara a cabo otra iteración de la valoración del riesgo con un contexto revisado.

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto.

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en donde la implementación de los controles se omite o se pospone.

Clasificación del Riesgo

Riesgo Estratégico: Está relacionado con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos y la definición de políticas.

Riesgo de Imagen: Es principalmente la percepción y la confianza que tiene la ciudadanía hacia la entidad.

Riesgo Operativo: Está relacionado con el funcionamiento y operatividad de los sistemas de información, la definición de los proceso, la estructura de la entidad y la articulación entre dependencias.

Riesgo Financiero: Se basa en el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejo de excedentes de tesorería y el manejo sobre los bienes.

Riesgo de cumplimiento: Esta asociado con la capacidad de la entidad para dar cumplimiento a los requisitos legales, contractuales, éticos y en general con su compromiso ante la comunidad.

Riesgo de Tecnología: Se relaciona con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales, futuras y el cumplimiento de la misión.

Identificación de Riesgos

Riesgo	Causas	Control
	-Posición inadecuada de los equipos.	-Las torres deben de estar a una altura de 5 cm de alto al piso.

Daños físicos en los Equipos Tecnológicos	-Derrame de líquidos.	-Capacitar a los funcionarios de no consumir bebidas ni alimentos en los puestos de trabajo.
	-Fallas o daños en los equipos de computo	Se debe hacer un cronograma mantenimiento preventivo cada seis(6) meses
	-No enfría los aires acondicionados en las dependencias	Se debe hacer un cronograma de mantenimiento preventivo
	-Fallas por defecto de fábrica.	Sugerir almacén que compren equipo corporativos o empresariales
	-Cumplimiento de la vida útil del equipo en el ambiente laboral.	-Solicitar cambio de equipo si ya lleva más de 5 años en funcionamiento dentro de la entidad.
	-Falta de repuestos para equipos y impresoras	Solicitar a almacén la compra de repuestos y equipos de computo
	-Falta de educación a los usuarios en el manejo de los equipos.	-Socialización de la Política de Seguridad de la información.
	-Falta de equipos de regulación de energía.	-Solicitar estabilizadores para regular los picos de energía.
Perdida de Conectividad	-Red de cableado obsoleta y falta de mantenimiento.	Solicitar almacén comprar cable nuevos
	-Arquitectura insegura de la red.	Asegurar los gabinetes y los puntos libres

	-switchs obsoletos	Solicitar almacén la comprar
Correos electrónicos de extraña procedencia	-Abrir o descargar información de correos no deseados o SPAM. -No generar una cultura de Seguridad de la Información.	-Socialización de la política y el Manual de Seguridad de la información. -Educar a los funcionarios en el tema de seguridad informática.
Perdida de información	-Desinformación a la hora de realizar la contratación o desvinculacion. -Falta de seguridad en las contraseñas. -Falta de autorización para la extracción de información generada en el equipo. -Ataques cibernéticos internos o externos. -Personal no capacitado en el tema de riesgos informáticos.	-Capacitar a las dependencias que debe informar a sistemas cuando contratan o se desvinculan los empleados para bloquear el usuario y salvaguardar la información. -Cambiar y no divulgar la contraseña que maneja para trabajar en el equipo o puesto de trabajo. -Conocimiento de la Política y el manual de Seguridad de la Información. -Contar con un antivirus para mitigar ataques cibernéticos y realice un una verificación de todos controles red interna y externa al equipo. -Capacitar el plan de riesgos de seguridad y Privacidad de la

		información.
	-Prestar los equipos informáticos a personal no autorizado.	-Sensibilizar a los funcionarios la importancia de no prestar de los equipo a personal no autorizada
	-Conectar dispositivos externos a los equipos.	Capacitar a los funcionarios de los manejos adecuados de los dispositivos externos
	-Falta de implementación de la política de escritorio del computador limpio.	Crear un política a los funcionarios del escritorio del computador limpio

Identificación de Controles Existentes

- La seguridad de la información es una obligación y responsabilidad de todos los funcionarios públicos y contratistas de la Alcaldia municipal de Girardot.
- En caso de daño de la información por diferentes eventualidades tal como ataques cibernético, físicos, ataques de virus, entre otros se debe de acudir inmediato a los Backups, en diferentes medios físicos y electrónicos.
- Todo equipo debe de estar protegido con firewall, antivirus, políticas dominio y todo lo relacionado con la protección de la información.
- Los equipos de la Alcaldia Municipal de Girardot cuentan con claves de acceso para que personas ajenas al grupo de trabajo no tengan acceso a ellos, estos se realiza con el objetivo de evitar perdida y daño de información.
- Ningún funcionario o contratista deberá de compartir las claves ya sea por medio telefónico o personal que fueron establecidas, ni permitir acceso no autorizado a los equipos de cómputo de la administración municipal. Para esto cada funcionario o contratista cuenta con un usuario de dominio asumiendo su responsabilidad sobre la información y por tanto debe tener precaución en uso de dicha cuenta.

- La Alcaldia Municipal de Girardot debe programar capacitaciones con cada uno de los funcionarios o contratistas, para que realicen un adecuado procedimiento en el manejo de la información y tenga un buen uso de las herramientas tecnológicas, mantenimiento de equipos, cambio de contraseñas, entre otros.

Evaluación de Riesgos

Este se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final el “Mapa de Color (Riesgo Inherente)”, con la cual se busca calificar los riesgos con los niveles de impacto y probabilidad.

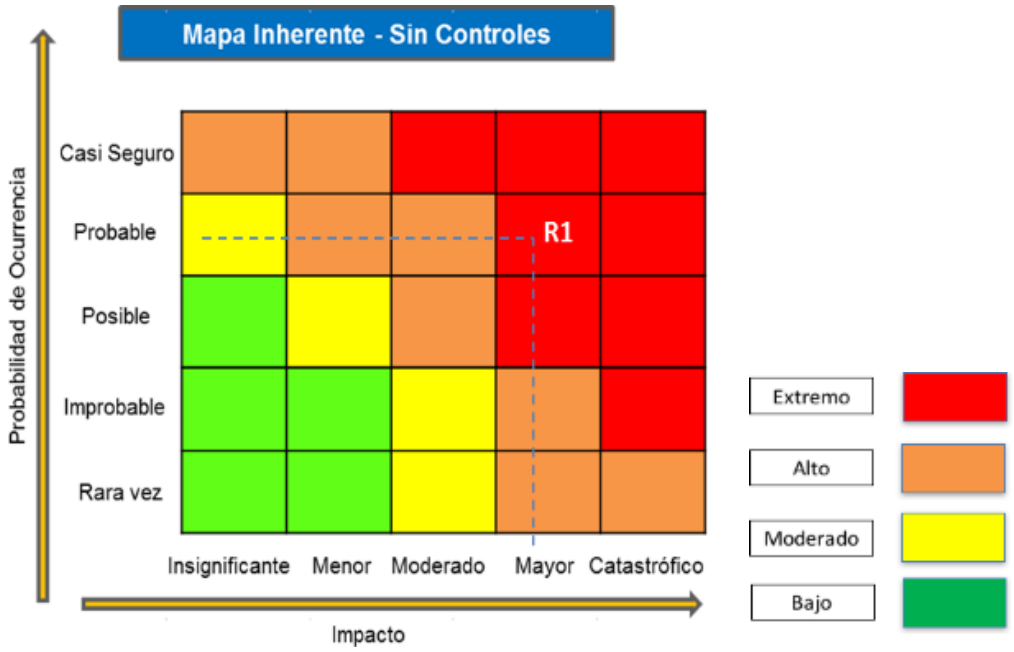

Imagen 3. Tomado de la Gestión riesgo y corrupción

La alcaldía municipal de Girardot evaluará el ejercicio de “tratamiento de riesgos y privacidad de la información”, por medio de seguimientos para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario. De esta forma conlleva, dado el caso, a evidenciar todas aquellas situaciones que pueden estar influyendo en la aplicación de las acciones de tratamiento.