ALCALDÍA DE
PAMPLONA

PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DE PAMPLONA

NORTE DE SANTANDER

2024

INTRODUCCIÓN

Es muy importante que la alcaldía de Pamplona implemente un plan de tratamiento de riesgos de seguridad y privacidad de la información, en el que se establezca un marco integral que aborde proactivamente los riesgos de seguridad y privacidad de la información. Buscando no solo salvaguardar los datos sensibles y garantizar la continuidad de las operaciones, sino también fortalecer la confianza pública y cumplir con las regulaciones legales y normativas relacionadas con la privacidad.

Teniendo en cuenta que la seguridad y privacidad de la información no son simplemente requisitos técnicos; son elementos fundamentales para la gobernanza efectiva y la entrega de servicios eficientes. La implementación de este plan no solo protegerá la información del municipio, sino que también sentará las bases para un gobierno transparente, responsable y centrado en la privacidad.

OBJETIVOS

Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para la Alcaldía de Pamplona.

Desarrollar e implementar medidas de seguridad proactivas para prevenir y mitigar amenazas cibernéticas, como ataques de malware, phishing o intrusiones, cifrados y controles de acceso, para garantizar que la información crítica y sensible del municipio sea accesible solo por personal autorizado, protegiendo así su confidencialidad.

Identificar las medidas de protección y remediación que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles informados en el Anexo A de la Norma Técnica Colombiana NTC- ISO/IEC 27001:2013 y los cuales ayuden al cumplimiento de los objetivos de cada Proceso y Procedimiento evaluado

Establecer y mantener prácticas de seguridad y privacidad que se alineen con las leyes y regulaciones pertinentes, asegurando que el municipio cumpla con los estándares legales para proteger la información y los derechos de privacidad de los ciudadanos.

ALCANCE

La Guía Metodológica de Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la Alcaldía de Pamplona.

ÁMBITO DE LA APLICACIÓN

La presente Guía aplica para el plan de tratamiento de riego de seguridad y privacidad de la información

REQUISITOS DE CALIDAD APLICABLE

Esta Guía da cumplimiento a los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información en la entidad.

DEFINICIONES

A continuación, se definen los términos Basados en la Norma ISO 27001. (ISO/IEC 27000) Para una mejor comprensión de la presente Guía Metodológica, se toman como referencia los términos y definiciones establecidos en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000 y el Modelo de Seguridad y Privacidad de la Información

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto. 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...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticidad: Propiedad de que una entidad es lo que afirma ser. Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

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.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de

la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los clientes de Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la Superintendencia Nacional de Salud debe ser clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

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.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Responsable de Seguridad Informática: En la alcaldía existe un comité comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al sistema de Gestión de la Seguridad de la información (SGSI) cuando este implementado.

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.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo. Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información;

Sistema de Gestión de la Seguridad de la Información: 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 del riesgo y de mejora continua.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

VALORACIÓN DE RIESGOS EN EL CONTEXTO DE LA ALCALDIA DE PAMPLONA A LOS ACTIVOS DE INFORMACIÓN

CONTEXTO DE LA ALCALDÍA DE PAMPLONA

La Alcaldía de Pamplona como meta principal busca fortalecerse como una entidad territorial administrativa que garantizará la prestación de los servicios públicos que determina la ley, así como la construcción de las obras necesarias con calidad para el progreso del municipio; promover el desarrollo integral para mejorar la calidad de vida de la comunidad, administrar los recursos del estado con transparencia, eficiencia y eficacia, con el desarrollo de planes, programas y proyectos encaminados al mejoramiento social, cultural , al ordenamiento y desarrollo de su territorio;

pero sobre todo implementar la seguridad y privacidad de la información que produce el municipio y garantizar una gestión eficaz de la información sensible.

CONTEXTO INTERNO

Servicios:

Protección a la información, protección al usuario y participación ciudadana

CONTEXTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

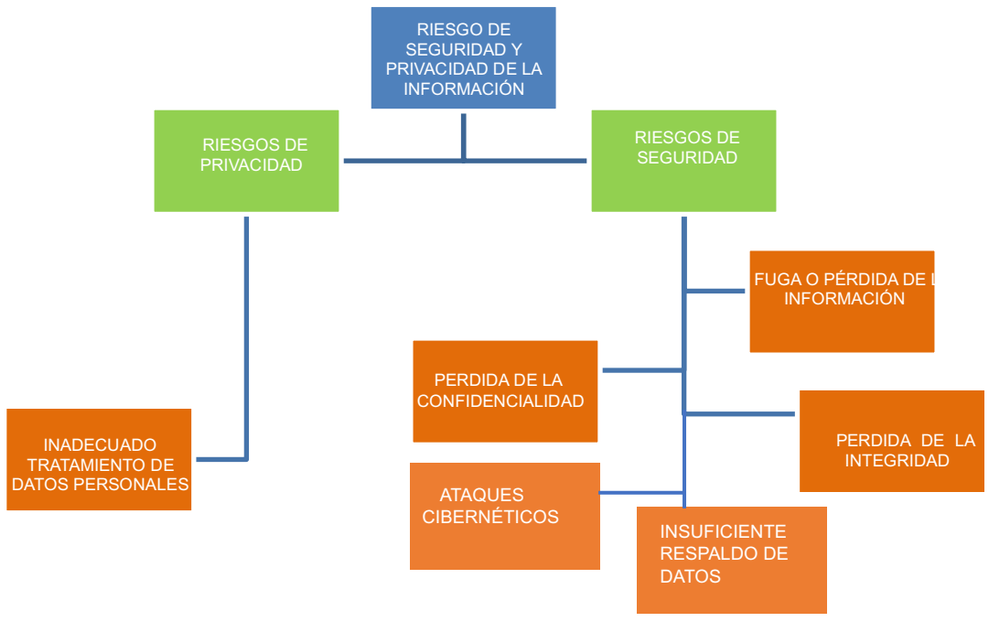
La información de La Alcaldía de Pamplona es decisiva para el desarrollo de sus procesos, su correcto desempeño dentro de su política y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de salida de eventos de riesgo de seguridad de la información y que pudiese parecer un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DEFINICIÓN DEL RIESGO

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "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". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información la alcaldía.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, la estrategia de administración de riesgos para el flujo de la información en los procesos busca diseñar una metodología ligera enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.



RIESGOS DE PRIVACIDAD

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como "Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las actividades y vulnerar la seguridad"; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información.

Los factores de riesgos que se encuentran identificados dentro de la entidad están los siguientes

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la realización del proceso de forma directa o indirecta.
Procesos	Contexto relacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.

Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Situaciones generadas por agentes externos, las cuales no son controlables por la entidad y que afectan de manera directa o indirecta el proceso.

ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDIA

Se identifican los activos de información, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores.

En la gestión de valoración del activo, se consideran los siguientes aspectos:

ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Datos de Configuración, Contraseñas, Datos de Control de Acceso, Registros de Actividad, Código Fuente.
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Equipos de Respaldo, Periféricos, Dispositivos Biométricos, Impresoras, Escáneres, Equipos Soporte de la Red , IP interconectados con tecnología Grandstream, IP y 4 NVR para los registros y administración, Lector de huellas biométrico IP para control de acceso, arquitectura Ethernet Router Board Mikrotic RB1100Ahx2.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Estándar, Navegador, Servidor, Correo Electrónico, Servidor de Correo Electrónico, Sistemas de Gestión de Bases de Datos, Software SOUL GT, Ofimática, Antivirus, Sistema Operativo, Backup o Respaldo,
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema)
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Contratistas, Proveedores.

Soportes de Información	**Dispositivos físicos electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red, Memorias USB, CDROM, DVD, Cinta Magnética, Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica,
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, paneles solares fibra óptica,
Instalaciones	Lugares donde residen los sistemas de información y comunicaciones.

Se establecen los niveles de riesgos teniendo una clasificación propia para de la alcaldía de Pamplona.

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Acción Requerida
Riesgo Extremo	Evadir el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Bajo	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones defectivas y preventivas.

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

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las Características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el

nivel de riesgo La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La alcaldía de Pamplona "evaluará el plan de tratamiento de riegos de seguridad y privacidad de la información", por medio de un monitoreo esencial 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, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos, el jefe de Control Interno y el personal de Apoyo TIC, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

ALCALDÍA DE PAMPLONA

PROCESO: Gestión Tecnológica y de la Información	**VIGENCIA: 2024**
RESPONSABLE:	**FIRMA DEL RESPONSABLE**

ACTIVIDADES	TEMAS	META POR ACTIVIDAD	MESES												RESPONSABLE
			1	2	3	4	5	6	7	8	9	10	11	12	
Realizar una evaluación detallada de los riesgos específicos para la seguridad y privacidad de la información en la entidad.	Realizar un estudio en las dependencias de la Entidad, que permita identificar las amenazas reales actuales.	Identificar las amenazas de casa dependencia.		X		X		X		X		X		X	OFICINA TIC
Identificar las amenazas que enfrentan los activos de información y tecnológicos mediante la elaboración de los mapas de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información de todos los Organismos de la Alcaldía de Pamplona	Realizar un estudio en las dependencias de la Entidad, que permita identificar las amenazas reales actuales.	Identificar las amenazas de casa dependencia.		X		X		X		X		X		X	OFICINA TIC
Implementar una políticas y ruta de procedimientos claros para la seguridad de la información.	Diseño de la política y ruta para la seguridad y privacidad de la información.	Crear y establecer la ruta de la seguridad y privacidad de la información que se adoptara por todas las dependencias de la alcaldía.		X	X	X	X	X							OFICINA TIC
Evaluar y gestionar los riesgos asociados con terceros que manejan información de la entidad, mediante acuerdos contractuales y evaluaciones de seguridad.	Evaluar el uso de la información de los contratistas.	Asegurarse que la información sensible sea tratada con confidencialidad.		X	X	X	X	X							
Implementar controles de acceso y gestión de identidad para garantizar que solo personal autorizado tenga acceso a la información crítica.	Determinar el personal designado para el uso de la información.	Prevenir la fuga de información.		X	X	X	X	X							

Fortalecer la cultura de seguridad de la información mediante difusión, sensibilización y capacitación de funcionarios, con el fin de dar tratamiento transparente y correcto de la información de todos los organismos y procesos de la Administración del Municipio de Pamplona.	Realizar periódicamente difusión, sensibilización o capacitación a los funcionarios con el fin de que cada uno tengamos claro el correcto manejo de la información.	Se espera trasmitir la ruta de control de cada uno de los funcionarios con respecto a toda la información de la alcaldía municipal.		X	X	X	X	X	X	X	X	X	X	X	OFICINA TIC
Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.	Realizar periódicamente revisión de que toda la información se encuentre en su debido orden para evitar pérdidas de las mismas	Se espera que la información de cada activo de la alcaldía sea protegida ante cualquier perdida que esta pueda causar		X	X	X	X	X	X	X	X	X	X	X	OFICINA TIC
implementar control de acceso a la información, sistemas y recursos de red.	Realizar mensualmente control de los accesos a los recursos de la red	Llegar a un control optimo del manejo de los recursos de red		X	X	X	X	X	X	X	X	X	X	X	OFICINA TIC
Reportar de forma inmediata al Área de sistemas o inventario cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.	Realizar periódicamente controles para prevenir riesgos que puedan afectar a los equipos	Lograr que los activos de la alcaldía no sufran daños		X	X	X	X	X	X	X	X	X	X	X	OFICINA TIC
Proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.	Realizar cada dos meses revisión de que las unidades de almacenamiento se encuentren bien protegidas y que contengan la informacion que se ha gusrdado	Lograr proteger las unidaes de almacenamiento que se encuenran a cargo de cada oficina			X		X		X		X		X		OFICINA TIC
Evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.	Realizar cada tres meses revisión de la informacion que contiene cada equipo al que se la ha asignado	Lograr contar con toda la informacion que se guarde en los equipos		X			X			X			X		OFICINA TIC

Realizar una charla en las oficinas de la alcaldía con el fin de hacer saber el plan de seguridad y el plan de riesgos para que cada funcionario tenga claro en que consiste	Realizar periódicamente charla en cada oficina de la alcaldía.	Llegar a feliz término y cumplir con lo establecido de los planes de privacidad, seguridad y el plan de riesgos		X	X	X	X	X	X	X	X	X	X	X	
Revisar periódicamente las políticas y prácticas de seguridad, y realizar mejoras continuas en función de las lecciones aprendidas y los cambios en el entorno operativo.	Realizar evaluaciones periódicas que permitan identificar malas prácticas.	Atender a tiempo las fallas que se puedan presentar.		X	X	X	X	X	X	X	X	X	X	X	

KLAUS FABER MOGOLLON

Alcalde Municipal

Nombres y Apellidos		Cargo	Firma
Proyectó:	JOHANNA HARO	PROFESIONAL DE APOYO GOBIERNO	
Reviso	GLADYS CAMERO PIMIENTO	ASESORA EXTERNA	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las disposiciones legales y/o técnicas vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma del Remitente.			