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

ALCALDIA MUNICIPAL DE GUATAPE

2021

INTRODUCCION

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 muy importante que las administraciones cuenten con un Plan de Gestión de Riesgos; por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La Alcaldía Municipal de Guatapé. Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la Alcaldía, donde se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

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 y recursos.

TABLA DE CONTENIDO

Pág.

Introducción

1. Objetivos

1.1 Objetivo General 5

1.2 Objetivos Específicos 5

Alcances y Limitaciones

2.1 Alcances 5

2.2 Limitaciones 5

3. Gestión de Riesgos

3.1 Importancia de la Gestión del Riesgo 6

3.2 Definición Gestión del Riesgo 7

3.3 Visión General para la administración del Riesgo de Seguridad de la Información…7

3.4 Identificación del Riesgo 7

3.5 Situación no deseada 8

4. Origen del plan de gestión de riesgo de SI 9

4.1 Propósito del plan de gestión de riesgo de SI 9

4.2 Identificación del riesgo 9

5. Análisis de vulnerabilidades 10

5.1 Descripción de vulnerabilidades 10

5.2 Matriz de vulnerabilidades y Mitigación del Riesgo 12

6. Propuesta de Seguridad 18

6.1 Plan seguro para el acopio de copias de seguridad 18

6.2 Plan de continuidad del negocio 19

6.3 Implementación de políticas 19

6.4 Plan de capacitación..... 19

6.5 Plan de transición de IPv4 a IPv6 20

Conclusiones

Bibliografía

1. OBJETIVOS

1.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la alcaldía Municipal de Guatapé.

1.2 Objetivos Específicos

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en la alcaldía municipal.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la alcaldía.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

Lograr el compromiso de la Alcaldía Municipal para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.

Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

2.2 LIMITACIONES

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Alcaldía Municipal de Guatapé.

3. GESTIÓN DE RIESGOS

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La alcaldía Municipal de Guatapé, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la alcaldía Municipal de Guatapé, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

3.2 DEFINICION GESTIÓN DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

3.3 VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Figura 1 Proceso para la administración del riesgo.

3.4 IDENTIFICACIÓN DEL RIESGO

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

3.5 SITUACION NO DESEADA

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información

4. ORIGEN DEL PLAN DE GESTION

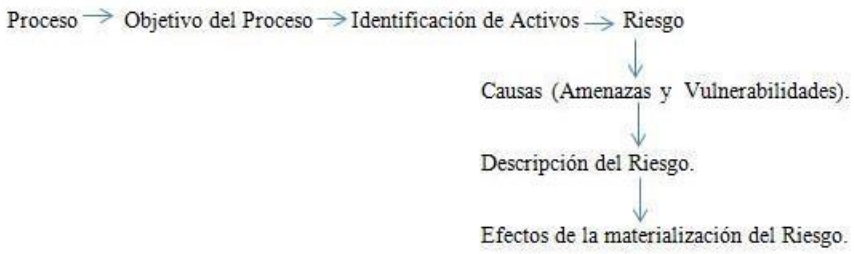
Debido al riesgo de pérdida de información es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las alcaldías y entidades públicas en el país. Es por ello necesario que la alcaldía municipal de Guatapé cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma alcaldía.

4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

4.2 IDENTIFICACIÓN DEL RIESGO



5. ANALISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Alcaldía de Guatapé se encontraron otras amenazas e impactos como los siguientes:

- La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte de la alcaldía tiene conexión WiFi y la señal se torna débil o no llega a algunas oficinas. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes. El internet lento y la perdida de señal afecta de forma directa los tiempos de producción laboral y desempeño de las funciones.

- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de la Alcaldía.

- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

- Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- En algunos papeles reutilizables se encontró información que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- En algunas secretarías de la alcaldía no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

- El Datacenter de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).

- La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.

- No hay control para el uso de memorias portátiles en los equipos de la Alcaldía, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en la alcaldía.

- No existe un Firewall para la red inalámbrica de la alcaldía.

- No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para la Alcaldía.

- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.

- Las copias de seguridad se están realizando únicamente en las secretarías y/o equipos donde se manejan software o sistemas de Información con un servidor dedicado a dicho propósito. Ésta solución no es óptima, ya que existe riesgo de pérdida de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas en el Datacenter ubicado dentro de la misma entidad.

- No existe un plan de continuidad que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la alcaldía. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)

- No se cuentan con los tipos de extintores adecuados para cada emergencia.

MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS CLASIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO	VIGENCIA O CUMPLIMIENTO
*Fallas eléctricas	Las conexiones no son suficiente. No cumplen con las exigencias. La infraestructura de la red se debe actualizar(hay cables sueltos, puntos de red que no funcionan)	Se han creado nuevos puestos de trabajo	Posible pérdida de la información	Riesgo tecnológico. Riesgo físico Riesgo humano	40	Riesgo moderado	Plantear nuevo diseño de la red	Vigencia 2023
Afectación de activos de información y activos informáticos	Desconocimiento de las políticas y normas de seguridad de la información	Falta de socialización. Falta de capacitación de la políticas y normas de seguridad	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal	60	Riesgo alto	Diseñar, socializar e implementar un manual de políticas de normas de seguridad de la información en la alcaldía.	Vigencia 2023
Pérdida de tiempo o productivo en funciones laborales	La red implementada no es la adecuada para la estructura física de la alcaldía y la cantidad de equipos informáticos. Las fallas en la señal de internet	Red inalámbrica ya que no hay suficientes puntos para cableado	Señal débil en oficinas. Retraso en los procesos	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal				

Incumplimiento de las actividades de seguridad de la información	El personal encargado de sistemas no es suficiente. El personal encargado de sistemas no está capacitado en instalaciones de red. No se siguen protocolos y normas para garantizar la seguridad de la información en la entidad.	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal	60	Riesgo alto	Contratar personal capacitado para asegurar el buen funcionamiento. Capacitar al personal de la alcaldía para el cumplimiento de procesos y actividades de seguridad de la información	Vigencia 2023
Confidencialidad e integridad de la información	En la alcaldía se trabaja en la campaña cero papel	Exposisición de datos importantes y reservados en e papel reutilizable.	Incumplimiento de la confidencialidad e integridad de la información	Riesgo de información	60	Riesgo alto	Socializar con los funcionarios de la entidad a cerca de las políticas de seguridad y confidencialidad de la información	Vigencia 2023
Pérdida total de la información	No se cuenta con los tipos de extintores adecuados para usarlos en caso de necesidad	No se cuenta con los tipos de extintores adecuados para usarlos en caso de necesidad	Extintores vencidos.	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal	40	Riesgo medio	Adquirir los extintores necesarios	Vigencia 2023
Pérdida de información	Los funcionarios no	No hacen copias	Posible pérdida de	Riesgo en el servicio.	40	Riesgo	Capacitar a funcionari	Vigencia 2023

	realizan copias de seguridad de los archivos mas relevantes e importantes. Uso de memorias y unidades extraibles	de seguridad No se hace control del uso	información Infección por virus	Riesgo de la información Riesgo tecnológico		important ante	os en copias de seguridad. Adquirir servidor para almacenar copias de seguridad. Adquisición de una nube de datos para almacenamiento de información. Crear nuevas cuentas de usuario con claves.	
Pérdida de la información y/o deterioro físico	La documentación en físico está siendo archivada en sitios no adecuados.	Continuar con la digitalización de la información	Deterioro de documentos	Riesgo de información	40	Riesgo importaten	Continuar con la digitalización	Vigencia 2021
Transición IPV4 a IPV6	No existe transición de protocolo de IP	No existe transición de protocolo de IP	No existe transición de protocolo de IP	Riesgo tecnológico	20	Riesgo bajo	Establecer normas para la transición de IPV4 a IPV6 debido a que todos los equipos informáticos soportan la nueva versión	Vigencia 2023

6. PROPUESTA DE SEGURIDAD

Implementar un firewall para la red que se utiliza en la alcaldía.

Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.

Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.

Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.

Socializar las políticas de seguridad y privacidad de la información con el personal de la alcaldía.

Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.

El personal de sistemas puede crear las cuentas y claves, socializando al personal de la alcaldía la creación de claves en forma correcta.

Asignar la función para dirigir la creación y el control de un sistema de seguridad y privacidad de la información en la Alcaldía junto con otras actividades propias del área.

Crear los procesos de la oficina de las TIC para la entidad.

6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Capacitar al personal en el almacenamiento de copias de seguridad de la información local manejada en las diferentes secretarías.

Obtener una nube dedicada para la información de la alcaldía con el fin de tener un respaldo en caso de accidentes en los servidores.

Contar con un plan alternativo que asegure la continuidad de la actividad en caso que ocurran incidentes graves.

Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

6.2 PLAN DE CONTINUIDAD

Socializar con los directivos, secretaría general y oficina de las TIC la importancia del Plan de Continuidad de la seguridad de la información, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

Detectar el riesgo

Plantear controles y efectuar las implementaciones respectivas.

Mitigar el riesgo.

Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

Política de copia de seguridad de datos

Procedimientos de almacenamiento fuera de la alcaldía

Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

6.3 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

Socialización y capacitación de temas de seguridad.

Ambiente con la seguridad física adecuada.

Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

6.4 PLAN DE CAPACITACIÓN

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

Detectar los requerimientos tecnológicos

Determinar objetivos de capacitación para personal

Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.

Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.

Evaluar los resultados de cada actividad.

6.6 PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de la alcaldía de Guatapé soportan la nueva versión de IP.

CONCLUSIONES

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Las políticas de seguridad de la información de la Alcaldía Municipal de Guatapé deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad

BIBLIOGRAFIA

GUIA DE GESTION DE RIESGOS. MINISTERIO. SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. MINISTERIO DE LAS TIC.

http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

JUAN SEBASTIAN PEREZ FLÓREZ
Alcalde Municipal