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

CONCEJO DISTRITAL DE CARTAGENA DE INDIAS

D.T.y C.

2022

PRESENTACION

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

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad de las funciones misionales, por este motivo, se ha visto la necesidad de desarrollar un análisis de nesgo do seguridad de la información aplicado en el Concejo Distrital de Cartagena , antes de iniciar con esto plan de gestión se ha revisado la situación actual de la corporación 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 con la seguridad de la información.

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

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 el Concejo Distrital de Cartagena.

1.2. Objetivos Específicos

Plantear modelos de reportes para su posterior uso en cada incidencia presentada en el Concejo Distrital de Cartagena.

• 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 el Concejo Distrital de Cartagena.

• 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

• Lograr el compromiso del Concejo Distrital de Cartagena 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.

3. GESTION DE RIESGOS

3.1. Importancia de la gestión de riesgos

El Concejo Distrital de Cartagena, 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, 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 de la entidad tras sufrir alguna pérdida o daño en la información de la entidad. Considerando la situación actual del Concejo Distrital de Cartagena, 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. Definición gestión del riesgo

La gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las posibilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse.

3.3. 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.

3.4. identificación de situaciones 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 DE RIESGOS

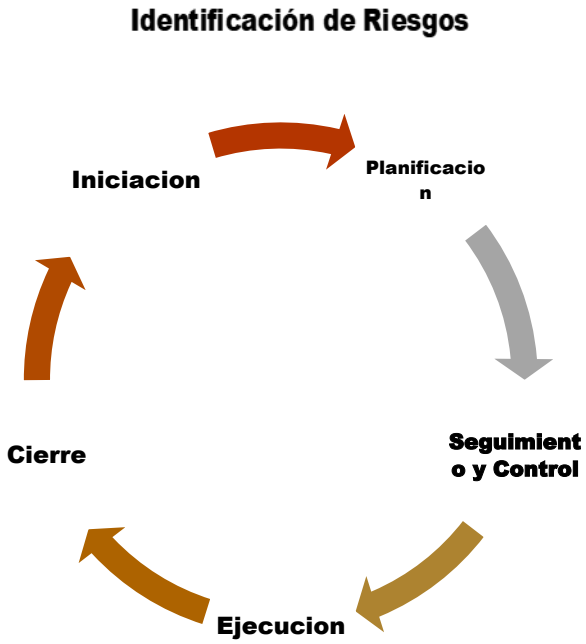
Debido al riesgo de pérdida de información es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

El gobierno nacional y el ministerio de las TICS han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las diferentes entidades públicas en el país. Es por ello necesario que el Concejo Municipal de Pasto cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades y a la población.

4.1. Propósito del plan de gestión 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, Limites 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 el Concejo Distrital de Cartagena se encontraron otras amenazas e impactos como los siguientes:

• Las políticas y normas de seguridad de la información existentes no son controladas, 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:
o Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de Líquidos afectan los activos de información y de informática.
o En algunos papeles reutilizables se encontró información que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

• 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.
• 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 del Concejo Distrital de Cartagena, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
• Se identifico un completo desconocimiento del tema de seguridad y privacidad de la información en el Concejo Distrital de Cartagena.
• 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.
• La mayoría de los documentos físicos que se manejan en la entidad no se han digitalizado por 10 tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

6. PROPUESTA DE SEGURIDAD

• 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.

• 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 del Concejo Distrital de Cartagena la creación de claves en forma correcta.

• Crear un plan del para la adquisición de la licencia del sistema ofimático Office y Sistemas Operativos para los equipos de la entidad.

7. PLAN SEGURO PARA LA CREACION DE COPIAS DE SEGURIDAD

- Capacitar de forma personal a los funcionarios del Concejo Distrital de Cartagena en el almacenamiento de copias de seguridad de la información local manejada en las diferentes dependencias.
- Contar con un plan alternativo que asegure la continuidad de la actividad en caso que ocurran incidentes graves.

8. IMPLEMENTACION DE POLITICAS DE SEGURIDAD PARA LA INFORMACION

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:

- Los temas de seguridad informático y de la información.
- Ambiente con la segundad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades.

IDENTIFICACIÓN DEL RIESGO					VALORACION DEL RIESGO DE CORRUPCION					MONITOREO Y REVISION				Responsable
PROCESO	OBJETIVO	RIESGO	CAUSAS	CONSECUENCIA	RIESGO INHERENTE				CONTROLES	FECHA	ACCIONES	RESPONSABLE	INDICADOR	
					PROBABILIDAD	IMPACTO	TOTAL	ZONA RIESGO						
INFORMÁTICA	Adquirir una página web como un canal de información para los ciudadanos sobre los servicios, informes y el control político	Página Web desactualizada	Inoportuna actualización de la página web	Información desactualizada para la toma de decisiones	3	20	60	Extrema	1.Actualizar la pagina web de acuerdo a la normatividad					Informatica
INFORMÁTICA	Copias de seguridad Backups	Generar copias de seguridad de la Información	No se realiza Backups en el proceso Informático	Perdida de información Hallazgos	3	10	30	Alta	Realizar un plan de copias de seguridad backups en unidades de almacenamiento cada 5 días en las dependencias mas influyentes					Informatica
INFORMÁTICA	Seguridad en el sistema informatico de la corporacion	Sistemas de información susceptibles de manipulación o adulteracion	1. Ausencia de cultura de auto control y auto gestión 2. Favorecimiento de intereses particulares en el cumplimiento de las metas	Imposibilidad de conocer o lider una base de datos basa en Información comecia y veraz	3	20	60	Extrema	1.Reunión con Desarrollo Organizacional para determinar acciones a seguir para desarrollar Plan de Contingencia 2. Inventario de Sistemas de Información y dependencias usuarias 3. validacion continua de la informacion generada					Informatica
INFORMÁTICA	Transparencia y publicidad de la informacion	Ocultar a la ciudadanía la información considerada pública	evitar cualquier tipo de control que pueda ejercido por la ciudadanía y las veedurias	1. vulneracion del derecho a la participacion ciudadana y vigilancia sobre la gestion de publica a los ciudadanos	2	20	40	Alta	plena observacia de los protocolos para la atencion de solicitudes de información establecidas en el procedimiento de atención y servicio al ciudadano					Informatica

Proyecto: FERNANDO HERRERA BARRIOS- Jefe Oficina de Informática