Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Instituto de Movilidad Pereira

Instituto de Movilidad
de Pereira

Contenido

1.1 Objetivo General

El objetivo de este plan es minimizar los riesgos de pérdida de activos de la información en el Instituto de Movilidad Pereira. Para ello, se establecen una serie de medidas de seguridad y privacidad que se deben implementar en todos los procesos y sistemas de información de la entidad.

1.1 Objetivos Específicos

- Establecer modelos de reportes para la gestión de incidentes de seguridad de la información.
- Implementar un proceso de gestión de eventos de seguridad de la información que permita detectar y tratar los incidentes de manera eficiente.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Identificar los principales activos de información a proteger en el Instituto de Movilidad Pereira.
- Identificar las principales amenazas que afectan a los activos de información del Instituto de Movilidad Pereira.
- Proponer soluciones para minimizar los riesgos a los que están expuestos los activos de información del Instituto de Movilidad Pereira.
- 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

2.1 Alcances

- El compromiso de la entidad es esencial para el éxito de cualquier plan de gestión de riesgos. En el caso del Instituto de Movilidad de Pereira, el compromiso de la alta dirección es fundamental para que el plan se implemente de manera efectiva.
- Designación de roles de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión de seguridad y privacidad de la información.
- La capacitación del personal es esencial para el éxito de cualquier plan de gestión de riesgos de seguridad de la información. El personal debe tener los conocimientos y las habilidades necesarias para identificar, evaluar y mitigar los riesgos a los que está expuesta la información de la entidad.

3. GESTIÓN DE RIESGOS

3.1 Importancia de la Gestión de Riesgos

En el ámbito empresarial, la seguridad de la información es un activo cada vez más valioso. Los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo, lo que hace que la información sea más vulnerable a los ataques y las amenazas.

En Risaralda, el Instituto de Movilidad de Pereira (IMP) sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno Digital. Estas iniciativas buscan que las entidades públicas se ajusten a modelos y estándares que permitan brindar seguridad a la información, dando cumplimiento al Decreto 1078 de 2015.

Sin embargo, el IMP aún enfrenta algunos desafíos en materia de seguridad de la información. Los riesgos más comunes son los desastres naturales, los riesgos inherentes relacionados con procesos inadecuados en el tratamiento de la información, el desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a la información. Esto es especialmente importante en el caso de las entidades públicas, que manejan información sensible sobre los ciudadanos.

Los riesgos más comunes a los que se enfrentan las organizaciones son los ataques dirigidos al software misional, que pueden afectar la disponibilidad, la integridad y la confidencialidad de la información.

Para prevenir estos riesgos, es importante tener un plan de gestión de riesgos de seguridad de la información. Este plan debe incluir los siguientes elementos:

- **Identificación de los riesgos:** Las organizaciones deben identificar los riesgos a los que está expuesta su información. Esto se puede hacer mediante una evaluación de riesgos.
- **Evaluación de los riesgos:** Las organizaciones deben evaluar los riesgos identificados para determinar su impacto y probabilidad.
- **Mitigación de los riesgos:** Las organizaciones deben implementar medidas para mitigar los riesgos identificados. Estas medidas pueden incluir controles de seguridad, políticas y procedimientos.

En el caso del IMP, 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.

Este plan debe incluir los siguientes elementos:

- **Conformación de un comité de seguridad de la información:** Este comité será responsable de liderar el desarrollo e implementación del plan.
- **Elaboración de un inventario de activos de información:** El inventario debe incluir todos los activos de información de la entidad, incluyendo sus características y riesgos asociados.
- **Evaluación de la madurez de la seguridad de la información:** La evaluación debe determinar el estado actual de la seguridad de la información de la entidad.
- **Desarrollo de un plan de acción:** El plan de acción debe establecer las acciones a realizar para mejorar la seguridad de la información de la entidad.

El desarrollo e implementación de un plan de gestión de riesgos de seguridad de la información es una inversión que vale la pena. Al reducir los niveles de riesgo, las organizaciones pueden proteger su información y garantizar la continuidad de sus operaciones.

3.2. Definición Gestión del Riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), que lo define como "la probabilidad de que un evento adverso ocurra y cause un impacto negativo en un objetivo".

3.3 Identificación del Riesgo

Riesgos estratégicos: Son los riesgos asociados con la forma en que se administra el Instituto.

- Impacto: Pueden afectar la misión, los objetivos estratégicos, las políticas y la estructura de la entidad.
- Ejemplos: Cambios en el entorno político o económico que afecten el cumplimiento de la misión del Instituto.
- Decisiones estratégicas erróneas que lleven a la pérdida de competitividad o a la disminución de la confianza de los ciudadanos.

Riesgos de imagen: Son los riesgos asociados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- Impacto: Pueden afectar la reputación, la credibilidad y la legitimidad de la entidad.
- Ejemplos: Casos de corrupción o malversación de recursos públicos.
- Fallos en la prestación de servicios que afecten a la ciudadanía.

Riesgos operativos: Son los riesgos asociados con el funcionamiento y operatividad de los sistemas de información, los procesos, la estructura de la entidad y la articulación entre dependencias.

- Impacto: Pueden afectar la continuidad de las operaciones, la eficiencia y la eficacia de la entidad.
- Ejemplos: Fallos en los sistemas de información que impidan el acceso a la información o la prestación de servicios.
- Procesos ineficientes que lleven a la pérdida de tiempo y recursos.

Riesgos financieros: Son los riesgos asociados con el manejo de los recursos de la entidad.

Impacto: Pueden afectar la liquidez, la solvencia y la sostenibilidad financiera de la entidad.

Ejemplos: Pérdidas financieras por causas naturales o accidentales.

Riesgos de cumplimiento: Son los riesgos asociados 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.

- Impacto: Pueden llevar a sanciones, multas, pérdida de reputación y daños a la imagen de la entidad.
- Ejemplos: Incumplimiento de las normas ambientales o de seguridad.

Riesgos tecnológicos: Son los riesgos asociados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras.

- Impacto: Pueden afectar la continuidad de las operaciones, la eficiencia y la eficacia de la entidad.
- Ejemplos: Fallos en los sistemas tecnológicos que impidan el acceso a la información o la prestación de servicios.

3.4 Situación no Deseada

Situación que puede causar daño o pérdida a la información, los sistemas o las operaciones del IMP

- 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

La información es el activo más valioso para cualquier organización, por lo que es esencial contar con un plan de gestión de riesgos de seguridad de la información que permita protegerla.

4.1 Propósito Del Plan de Gestión de Riesgo de la Seguridad de la Información.

Este plan debe identificar, evaluar y mitigar los riesgos a los que está expuesta la información, con el objetivo de garantizar su disponibilidad, integridad y confidencialidad.

- **Identificación de riesgos:** Esta etapa consiste en identificar todos los riesgos a los que está expuesta la información, tanto internos como externos.
- **Evaluación de riesgos**: Esta etapa consiste en evaluar la probabilidad e impacto de cada uno de los riesgos identificados.
- **Mitigación de riesgos:** Esta etapa consiste en implementar medidas para reducir la probabilidad o el impacto de los riesgos identificados.

La implementación de un plan de gestión de riesgos de seguridad de la información proporciona a las organizaciones los siguientes beneficios:

- **Protección de la información:** El plan ayuda a proteger la información de la organización de los riesgos a los que está expuesta.
- **Reducción de costes:** El plan ayuda a reducir los costes asociados a la pérdida de información, como costes de recuperación, costes de interrupción de las operaciones y costes de multas o sanciones.
- **Mejora de la reputación:** El plan ayuda a proteger la reputación de la organización en caso de que se produzca una pérdida de información.

5. ANALISIS DE VULNERABILIDADES

5.1 Descripción de Vulnerabilidades

La protección de la información digital de la entidad se ve amenazada por una serie de factores, tanto internos como externos.

Entre los factores internos, se encuentran los siguientes:

- **Inadecuada planificación y gestión de la infraestructura de red:** Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. Esto puede provocar interrupciones en el servicio o la pérdida de información.
- **Cables de energía sueltos o insuficientes:** 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. Esto puede provocar daños a los equipos o la pérdida de información.

- **Incumplimiento de las políticas y normas de seguridad de la información:** Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal. Esto provoca el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos como de la información física y digital.

Algunos ejemplos de incumplimiento de las políticas de seguridad de la información son:

- **Uso de bebidas y alimentos cerca a los equipos de cómputo:** Esto puede provocar derrames de líquidos que dañen los equipos o la información almacenada en ellos.
- **Almacenamiento de información personal en papeles reutilizables:** Esto puede provocar la pérdida de confidencialidad de la información.
- **Falta de equipos de cómputo suficientes para el uso de todo el personal:** Esto puede provocar el uso compartido de equipos, lo que aumenta el riesgo de pérdida de información.
- **Llevar información en memorias o discos duros portátiles personales:** Esto puede provocar la salida de la información de la entidad, lo que aumenta el riesgo de pérdida o robo.
- **Ausencia de control para el uso de memorias portátiles en los equipos del Instituto:** Esto puede provocar la pérdida de información por virus o daños irreparables del hardware.

Entre los factores externos, se encuentran los siguientes:

- **Falta de actualización del firewall:** Los firewalls son dispositivos de seguridad que protegen las redes de los ataques externos. Es importante mantenerlos actualizados para evitar que sean vulnerables a nuevos ataques.
- **Falta de un plan de continuidad de negocio:** Un plan de continuidad de negocio permite reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la entidad. En caso de incendio o desastre natural, la falta de un plan de continuidad de negocio puede provocar la pérdida de información de los servidores.

Para mitigar los riesgos a los que está expuesta la información digital de la entidad, es necesario implementar las siguientes medidas:

- **Mejorar la planificación y gestión de la infraestructura de red:** Se deben realizar estudios para determinar la cantidad de puntos de red necesarios en cada oficina y garantizar que los cables de energía estén en buen estado y cerca a los escritorios.
- **Mejorar la seguridad de los cables de energía: Se** deben asegurar los cables de energía para evitar que se desconecten accidentalmente.
- **Socializar las políticas y normas de seguridad de la información con todo el personal:** Se deben realizar capacitaciones para que el personal conozca las políticas y normas de seguridad de la información y las aplique en su trabajo diario.
- **Adoptar medidas para evitar el incumplimiento de las políticas de seguridad de la información:** Se pueden establecer controles para supervisar el cumplimiento de las políticas de seguridad de la información, como la instalación de cámaras de seguridad o la realización de auditorías.
- **Actualizar los firewalls:** Se deben actualizar los firewalls de forma periódica para evitar que sean vulnerables a nuevos ataques.

- **Desarrollar un plan de continuidad de negocio:** El plan de continuidad de negocio debe incluir medidas para proteger la información de los servidores en caso de incendio o desastre natural.

6. PROPUESTA DE SEGURIDAD

Se recomienda adquirir equipos FortiWiFi 100 o superior para proteger la red de la entidad.

- Mayor rendimiento
- Mayor seguridad
- Mayor facilidad de gestión

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 del instituto.

6.1 Plan Seguro para el Acopio de Copias de Seguridad

Adquirir un espacio en la nube con características específicas para el almacenamiento de copias de seguridad:

- El espacio en la nube debe estar ubicado en un centro de datos de alta disponibilidad.
- El espacio en la nube debe tener una capacidad suficiente para almacenar todas las copias de seguridad de la entidad.
- El espacio en la nube debe ofrecer un nivel de seguridad adecuado para proteger la información de la entidad.

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

- El plan alternativo debe incluir medidas para proteger la información de la entidad en caso de desastre natural o incendio.
- El plan alternativo debe incluir medidas para permitir la recuperación de la información en caso de pérdida o deterioro de los sistemas informáticos.

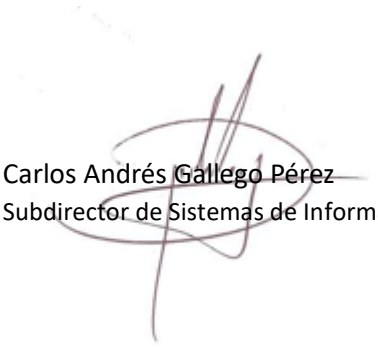
6.2 Implementación de Políticas de Seguridad para la Información

El análisis realizado permitió identificar que las políticas de seguridad de la información son desconocidas y poco se cumplen en el IMP. Por lo tanto, es necesario integrarlas con el documento actual, teniendo en cuenta las siguientes recomendaciones:

- **Socialización y capacitación:** Es importante que todos los colaboradores de la organización conozcan las políticas de seguridad y cómo cumplirlas. Para ello, se deben realizar acciones de socialización y capacitación periódicas, utilizando medios y formatos adecuados a los diferentes públicos.
- **Seguridad física:** La seguridad física de los activos de información es fundamental para protegerlos de amenazas externas. Se deben implementar controles de seguridad físicos, como accesos controlados, videovigilancia y sistemas de alarmas.
- **Respaldos:** Los sistemas de respaldo son necesarios para recuperar la información en caso de pérdida o daño. Se deben implementar sistemas de respaldo que garanticen la integridad y disponibilidad de la información.

6.3 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 del instituto soportan la nueva versión de IP



Carlos Andrés Gallego Pérez
Subdirector de Sistemas de Información y Telemática