



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

INTRODUCCIÓN

La gestión de los riesgos de seguridad y privacidad de la información es el proceso mediante el cual se busca reducir la pérdida y protección de la información, permitiendo conocer las debilidades que 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 del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en el IMCTC. Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la empresa, 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.

OBJETIVOS

Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad de la información que permita minimizar riesgos de pérdida de activos de la información en el IMCTC.



Objetivos Específicos

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en el IMCTC.
- 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 IMCTC.
- 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

ALCANCES Y LIMITACIONES

Alcances

Lograr el compromiso del IMCTC 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.

Limitaciones



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

GESTIÓN DE RIESGOS

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.

El IMCTC, 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 del IMCTC, 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.

Definición 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”.

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.

Situación 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

ORIGEN DEL PLAN DE GESTION

Debido a que el IMCTC no tenía un área de sistemas conformada y se evidenció que no existen procesos asignados a dicha área entre otras vulnerabilidades que



se encontraron en el sistema actual, 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.

La situación actual del sistema de seguridad de la información en la entidad se encuentra planteado en el Diagnostico de seguridad y privacidad de la Información con fecha de junio de 2019.

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

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, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

ANALISIS DE VULNERABILIDADES

Descripción de Vulnerabilidades

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



- No hay zona WiFi
- 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 del IMCTC.
- 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.
- No hay políticas y normas de seguridad de la información
- 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 personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
- En algunas áreas 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.
- No hay un Datacenter para centralizar y almacenar la información.
- No existen cuentas de usuario y claves para el acceso de los recursos informáticos, en equipos compartidos.
- 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 Instituto, 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 el instituto.



- 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.
- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a pérdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
- No existen procesos de copias de seguridad establecidos. 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.
- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones del Instituto. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores).