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 el ciclo de vida de los datos.

Cualquier sistema de información es susceptible de riesgos a la seguridad y privacidad de los datos y es de gran importancia que toda entidad u organización cuente con un plan de gestión de riesgos para garantizar la continuidad de los servicios. Por este motivo, El Instituto Municipal de Cultura y Turismo de Cajicá se ha visto en la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado a sus procesos.

Este plan permite identificar el nivel de riesgo en que se encuentran los activos de información mediante la valoración de la seguridad existente a nivel de Hardware y Software, y la permanente capacitación al personal para seguir las normas y procedimientos referentes a la seguridad de la información.

Alcance

Que los funcionarios y contratistas del IMCTC comprendan los riesgos inherentes al uso de herramientas informáticas aplicadas a la administración de la información institucional.

Todas las plataformas y herramientas con las cuales el IMCTC, en el desarrollo de sus actividades, recopila, almacena y procesa información.

Objetivos

Objetivo General

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

Objetivos Específicos

Objetivo 1: Promover la centralización de datos a través del uso de las herramientas informáticas institucionales implementadas y/o controladas por el IMCTC, para facilitar los procesos de backup y restauración de datos.

Objetivo 2: Registrar, clasificar, cuantificar y evaluar el reporte de incidentes que involucren riesgos de seguridad a la información, e identificar los puntos críticos que se deben atender con mayor prioridad.

Objetivo 3: Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de información.

Objetivo 4: Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el Plan de Tratamiento de Riesgos y Privacidad de la Información.

Definiciones básicas

• **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

• **Amenaza**: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

• **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

• **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo. • Impacto: son las consecuencias que genera un riesgo una vez se materialice.

• **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Marco Normativo

- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 1266 de 2008. Disposiciones generales Habeas Data.
- Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014.Transparencia y Acceso a la información Pública Nacional.
- Decreto 4170 de 2011. Creación de la ANCP-CCE.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 1083 de 2015. Único Reglamentario del Sector Función Pública, con las modificaciones y adiciones introducidas a partir de su fecha de su expedición.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo con las modificaciones y adiciones introducidas a partir de su fecha de su expedición

Diagnóstico

El IMCTC cuenta con servidores para el almacenamiento y procesamiento de datos institucionales y herramientas de software para el manejo de dicha información. Las herramientas de colaboración habilitadas son: Servidor de archivos, Correo Electrónico de 10 GB, Calendario Web, Almacenamiento Cloud de 20 GB, Herramienta de Encuestas, Mesa de Ayuda, Red Social SIACCA, Systema ERP Sysman y plataforma de e-Learning Q10.

Estos sistemas de información requieren una vigilancia permanente y registros de entrada y salida de datos para adelantarse a los posibles riesgos en la seguridad de la información almacenada o procesada. Así mismo, se debe capacitar a funcionarios y contratistas en la aplicación de buenas prácticas en el manejo de información.

Componentes del Plan

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información descrito en este documento, requiere para su implementación, tres componentes fundamentales:

Socialización de Información. Él envió de información digital periódica pretende incentivar el uso de las herramientas informáticas institucionales, mediante la socialización de las plataformas disponibles, características instaladas, solución de inquietudes y el apoyo permanente a los funcionarios y contratistas como usuarios del sistema.
Funcionarios y contratistas. Todos los funcionarios y contratistas del IMCTC deben usar de manera única y permanente las herramientas provistas por el Instituto para el desarrollo de sus labores contractuales y reportar a través del correo soporte@culturacajica.gov.co los incidentes y/o situaciones que se puedan presentar en la interacción con las mismas. De esta forma se garantiza el almacenamiento adecuado de los datos y la centralización de las solicitudes mediante un servicio controlado.

Mesa de ayuda. Los incidentes reportados a través del correo mencionado anteriormente son el insumo de la Mesa de Ayuda para el registro, gestión y solución de los eventos que puedan involucrar riesgos de acceso, integridad o filtración de los datos almacenados por el IMCTC o que sean procesados en las herramientas implementadas en sitio o contratadas con terceros. El dato exportado de manera periódica por el servicio de Mesa de Ayuda permitirá la clasificación cualitativa y cuantitativa de los riesgos a los activos de información y la asignación de prioridades para su mitigación.

Plan de Acción Anual

ESTRATEGIAS

- Se realizará envío de información por correo electronico que muestren las características de las herramientas y el uso correcto de cada una, buscando que los usuarios solo usen herramientas controladas por el IMCTC.
- Socializar el uso de la Mesa de Ayuda como el servicio adecuado para el reporte de incidentes relacionados con el uso de las herramientas informáticas institucionales y los datos contenidos o procesados por estas.
- Establecer controles que mitiguen los riesgos de seguridad informática que sean detectados de manera temprana por el sistema de seguridad del IMCTC.
- Graficar de manera periódica la cuantificación de incidentes que involucren riesgos a la seguridad y privacidad de la información institucional, usando la información exportada de la Mesa de Ayuda.

META: Implementar y mantener un servicio de información con características de usabilidad e integridad para los datos institucionales, que mantenga niveles de seguridad y privacidad acordes a las actividades del IMCTC.

INDICADOR: Cada objetivo se acompaña de uno o varios indicadores para su gestión y control de cumplimiento. A continuación, se mencionan los indicadores establecidos para el Proceso de Gestión de Recursos Tecnológicos con vigencia 2024.

- Adopción de herramientas tecnológicas
- Gestión de solicitudes de soporte y/o asistencia técnica

CRONOGRAMA:

ACTIVIDAD	RESPONSABLE	ENTREGABLE	FECHA DE INICIO	FECHA DE FINALIZACIÓN	PERIODICIDAD
Socialización de información por Correo Electrónico	Contratista Área de tecnología	Registro de Envíos	01/02/2024	30/12/2024	Mensual
Validación y seguimiento de servicios informáticos	Contratista Área de tecnología	Registro de Seguimiento	01/02/2024	30/12/2024	Mensual
Solución de Incidentes de Mesa de Ayuda	Contratista Área de tecnología	Registro mensual de Tickets	01/02/2024	30/12/2024	Mensual

Referencias

Guia de Gestión de riesgos -Seguridad y Privacidad de la información
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf