INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE CAJICÁ

Plan de Seguridad y Privacidad de la Información

JUSTIFICACIÓN

El IMCTC busca salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información, con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de Seguridad de la información física y digital de acuerdo a la caracterización de los Usuarios tanto internos como externos.

OBJETIVOS

OBJETIVO GENERAL

Establecer las políticas para garantizar la administración, manejo y control de la seguridad y privacidad de la información del IMCTC.

OBJETIVOS ESPECÍFICOS

- Establecer políticas de seguridad y privacidad de la información del IMCTC.
- Identificar los niveles de cumplimiento y alcance de las políticas de seguridad y privacidad de la información.
- Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la Información

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ALCANCE

Esta política aplica a toda la entidad, funcionarios, contratistas y terceros del IMCTC.

NIVEL DE CUMPLIMIENTO

- Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política. A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- El IMCTC, protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
- El IMCTC protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El IMCTC protege su información de las amenazas originadas por parte del personal.
- El IMCTC protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El IMCTC controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos información, sistemas y recursos de red.

- El IMCTC garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El IMCTC garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El IMCTC garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- El IMCTC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN

La seguridad y privacidad de la información se entiende como la preservación de las siguientes características:

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Dirección: Calle 1A # 0-40
Cajicá - Cundinamarca- Colombia
Teléfonos: (57+1) 310 584 4637 - 310 205 6145
Correo electrónico: pqr@culturacajica.gov.co
página web: www.culturacajica.gov.co

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Por tanto, a los efectos de una correcta interpretación del presente plan, se realizan las siguientes definiciones:

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: se refiere a un conjunto independiente de recursos de Información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

CONTROL DE ACCESO

Política de acceso a redes y recursos de red

El técnico operativo o ingeniero de sistemas del IMCTC como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

El proceso Gestión de TIC debe asegurar que las redes inalámbricas del IMCTC cuenten con métodos de autenticación que evite accesos no autorizados.

El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de éstos.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del IMCTC deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Política de administración de acceso de usuarios

El IMCTC establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Política de control de acceso a sistemas de información y aplicativos

El IMCTC como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El área de TI, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que éstos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Políticas de seguridad física

El IMCTC, provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

Política de seguridad para los equipos

El IMCTC para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

- El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del IMCTC.
- El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de las plataformas tecnológicas de la entidad, redes de datos, equipos de cómputo y demás dispositivos disponibles al servicio del instituto.
- El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga

de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

- El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.
- El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.
- El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones del IMCTC cuente con la autorización documentada y aprobada previamente por el área de sistemas.
- El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.
- El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del IMCTC.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las Instrucciones técnicas que proporcione el proceso Gestión de TIC.

- Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad del IMCTC, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por el personal autorizado o de apoyo al proceso de Gestión de TIC.
- Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados atendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al Jefe inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

Política de uso adecuado de internet

El IMCTC consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios

para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

- El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
- El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
- Los usuarios del servicio de Internet del IMCTC, deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles
- asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios
- interactivos o mensajería instantánea como Facebook, Whatsappweb, Kazaa, MSN,
- Yahoo, Skype, Instagram y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del instituto.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música,
- películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e
- imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad del IMCTC, por parte de los funcionarios con terceros.

PRIVACIDAD Y CONFIDENCIALIDAD

POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, el IMCTC propende por la protección de los datos

personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales el IMCTC, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, el IMCTC exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización

DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

El IMCTC con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, ha decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

Política de continuidad, contingencia y recuperación de la información

El IMCTC proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

COPIAS DE SEGURIDAD

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias del IMCTC deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad.

La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

CUMPLIMIENTO Y NORMATIVIDAD LEGAL.

Controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad. Garantizar que la gestión de la seguridad dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad de la información, uso inadecuado de recursos de procesamiento de información, uso de criptografía y recolección de evidencias.

Así mismo deberá garantizarse que el direccionamiento y los controles relacionados con la seguridad de la información se cumplen y son compatibles técnicamente con los diferentes ambientes y tecnologías. Se debe garantizar la posibilidad de llevar a cabo auditorias, manteniendo los registros necesarios, para que éstas respondan

adecuadamente a la disminución del riesgo de discontinuidad de cada tarea o servicio propio del IMCTC.

EVALUACIÓN DE RIESGOS

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Instituto.

ADMINISTRACIÓN DE RIESGOS

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

RESPONSABLE DE SEGURIDAD INFORMÁTICA

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del instituto que así lo requiera, profesional con experiencia en seguridad informática.

INCIDENTE DE SEGURIDAD

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

CORREO ELECTRÓNICO MASIVO

El correo electrónico masivo se refiere a cualquier mensaje de correo electrónico enviado a una larga lista de destinatarios que tiene un contacto idéntico para cada persona. Ejemplos típicos de correo electrónico masivo son boletines de noticias, listas de discusión y actualizaciones de la compañía. El correo electrónico a granel puede ser enviado por una entidad comercial, como una empresa de automóviles que envía un boletín a las personas que son dueños de sus vehículos, o un restaurante envía cupones u ofertas especiales. También puede ser enviado por un individuo a través de un mensaje enviado por un miembro de un grupo de discusión que va a todos los otros miembros del grupo

Dirección: Calle 1A # 0-40
Cajicá - Cundinamarca- Colombia
Teléfonos: (57+1) 310 584 4637 - 310 205 6145
Correo electrónico: pqr@culturacajica.gov.co
página web: www.culturacajica.gov.co