INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE CAJICÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Inscultura con el propósito de 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/o, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

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

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas.

- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos adecuados.

Adicionalmente, debe considerarse los conceptos de:

- **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.

- **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.

OBJETIVOS

- Preservar, proteger y administrar de forma eficiente la información del Inscultura junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento

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

de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información del Inscultura, para asegurar su sostenibilidad y el nivel de eficacia.

POBLACIÓN OBJETIVO

El Plan de Privacidad y Seguridad de la Información está dirigido al personal del Inscultura, tanto de la planta de personal como los contratistas.

CANALES DE COMUNICACIÓN

El Plan de Seguridad y Privacidad de la Información será difundida a través de la página web del Inscultura.

NIVEL DE CUMPLIMIENTO

El Inscultura ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar total cumplimiento de la política.

PRINCIPIOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI:

1. El Inscultura ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de funcionarios provisionales, funcionarios con carrera administrativa, funcionarios con libre nombramiento y contratistas.
3. El Inscultura, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, incluyendo los datos personales conforme lo define la Ley 1581 de 2012 y las normas que complementen, definen o reglamentan.
4. El Inscultura, protegerá la información creada, procesada, transmitida o resguardada

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

por sus procesos, 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.

5. El Inscultura, protegerá su información de las amenazas originadas por parte del personal.

6. El Inscultura, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. El Inscultura, controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. El Inscultura, implementará control de acceso a la información, sistemas y recursos de red. Política general del modelo de seguridad y privacidad de la información.

9. El Inscultura, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. El Inscultura, garantizará 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.

11. El Inscultura, garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. El Inscultura, 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, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

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

INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE CAJICÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN

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 Inscultura.

Objetivos Específicos

- 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.
- Identificar las principales amenazas que afectan a los activos informáticos.
- 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

Alcance

- 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.

Gestión de riesgos

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

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

causa daño a la organización".

Visión General para la Administración del Riesgo de Seguridad de la Información

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

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

Errores cometidos por los usuarios.

Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, 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:

✓ Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- ✓ En papel reutilizable se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
- ✓ Actualmente se está implementando un sistema de Almacenamiento de información centralizado y privado.
- ✓ Hay información que circula en en memorias usb 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 Inscultura, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- ✓ Se evidencia desconocimiento por parte de los usuarios de los temas claves en materia de seguridad y privacidad de la información.
- ✓ 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 perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
- ✓ No todos los equipos ejecutan un sistema de sincronización de información y Backup

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