INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA

Manual de Políticas de Seguridad Informática
INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA

M-GT-01 VERSIÓN 02

Tabla de contenido

Introducción

La información es un activo de alto valor para el Instituto de Cultura y Patrimonio de Antioquia. A medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos.

El presente manual contiene los lineamientos que rigen la actuación de los Servidores públicos y contratistas del Instituto de Cultura y Patrimonio de Antioquia, en cumplimiento de las disposiciones legales vigentes, con el objeto de salvaguardar la información de la entidad.

Las políticas que aplican específicamente al personal de equipo de trabajo de informática se presentan en el numeral 2 del presente manual.

El manual de políticas contiene lineamientos y directrices tanto de seguridad de la información como de seguridad informática. La adopción de los dos enfoques busca afrontar integralmente las amenazas que pueden comprometer a la información de la entidad.

Propósitos

- Formalizar el compromiso del Instituto de Cultura y Patrimonio de Antioquia frente a la seguridad informática.
- Definir los lineamientos de seguridad que deberán seguirse para proteger la información al interior del Instituto de Cultura y Patrimonio de Antioquia.
- Fundamentar la futura definición de procedimientos, protocolos y estándares de seguridad informática en la entidad.

Principios

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

- Promover comportamientos de seguridad responsables.
- Exhortar las actuaciones profesionales y éticas.
- Promover una cultura positiva para la seguridad.
- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Promover la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.

- Proteger la organización.
- Soportar el actuar de la entidad.
- Enfocarse en la organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad
- Concentrarse en aplicaciones organizacionales críticas.
- Buscar el desarrollo sistemas de información de forma segura.

Roles y responsabilidades asociadas a la presente política

Área de Sistemas

- Formular y mantener actualizadas las políticas de seguridad informática para toda la entidad.
- Revisar, aprobar y mantener el cumplimiento de las políticas, normas y procedimientos de seguridad informática.

Subdirectores

- Asegurar que los servidores públicos y contratistas bajo su responsabilidad conozcan, entiendan y atiendan las políticas contenidas en el presente manual.
- Aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad informática dentro de los procesos del Sistema Integrado de Gestión que lideren.

Servidores públicos y contratistas

- Conocer y cumplir las políticas indicadas en este manual.
- Reportar las infracciones o incumplimientos que identifique.
- Apoyar a otros servidores en el cumplimiento de las políticas indicadas en este manual

Subdirector administrativo y Financiero

- Dirigir el plan estratégico de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad informática en el marco del cumplimiento de las políticas definidas y aprobadas.
- Identificar oportunidades para la mejora de las políticas de seguridad informática en función de las necesidades de la entidad y de los riesgos que sean identificados.

Cumplimiento de requisitos legales y regulatorios

El presente manual de políticas fue construido para proteger la información y la plataforma de tecnologías de información del Instituto de Cultura y Patrimonio de Antioquia; en ningún momento la aplicación de las políticas de seguridad informática podrá dañar los derechos fundamentales de las personas como el derecho a la intimidad o el derecho a la vida, la salud o la seguridad.

Así mismo, las políticas de seguridad informática fueron definidas de conformidad a lo establecido en:

- La Ley 1712 de 2014. *Ley de transparencia y del derecho de acceso a la información pública nacional.*
- La Ley 1581 de 2012 y decreto 1377 de 2013. *Ley de protección de datos personales.*
- La Ley 1273. *Ley de delitos informáticos y la protección de la información y de los datos.*
- El Decreto 2693 DE 2012. *Lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia.*
- La Ley 527/1999. *Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.*

Sanciones y proceso disciplinario

El desacato o incumplimiento a las presentes políticas por parte de un servidor público del Instituto de Cultura y Patrimonio de Antioquia puede acarrear acciones disciplinarias. Dichas medidas se impartirán en coherencia con la ley vigente y los reglamentos internos de trabajo del Instituto de Cultura y Patrimonio de Antioquia.

Una infracción o falta de estas políticas por parte de un contratista puede generar la terminación de su contrato con el Instituto de Cultura y Patrimonio de Antioquia.

Definiciones

Borrado seguro: Procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.

Centro de Servicios Informáticos - CSI: Equipo responsable de gestionar las solicitudes de servicio relacionadas con la plataforma de tecnologías de información del Instituto de Cultura y Patrimonio de Antioquia.

Contratista: Trabajador que hace parte de una empresa o entidad contratada por el Instituto de Cultura y Patrimonio de Antioquia para la prestación de sus servicios.

Correo masivo: Expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que forme parte de los dominios "@culturantioquia.gov.co".

Criterio de seguridad informática del Instituto de Cultura y Patrimonio de Antioquia: Conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.

Derechos / Privilegios de acceso: Conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio de red, aplicativo, datos).

Dispositivos móviles: Son aparatos con algunas capacidades de procesamiento y de conectividad. Su principal característica es su movilidad. Los dispositivos móviles abarcan una gran variedad de equipos como: teléfonos inteligentes, asistentes digitales personales (PDA), tabletas, y computadoras portátiles.

Entidad: Término que se usa en el presente documento para identificar el Instituto de Cultura y Patrimonio de Antioquia cuando sea conveniente.

Equipos de trabajo de informática: Expresión que se usa en el presente documento para identificar a los equipos de trabajo del Instituto de Cultura y Patrimonio de Antioquia que son responsables de desarrollar, desplegar, mantener y administrar las plataformas de tecnología de información. Esta expresión abarca a los integrantes de la Dirección de Informática y personal de otras áreas de la entidad con alguna de las responsabilidades mencionadas.

Equipo de seguridad de la información: Grupo funcional adscrito a la Dirección de Informática, cuya función primordial es la de gestionar la seguridad para el alcance previsto del SGSI del Instituto de Cultura y Patrimonio de Antioquia, buscando que el nivel de riesgo de la información de la entidad permanezca en niveles aceptables.

Evento de seguridad informática: Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad informática, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.[1]

Incidente de seguridad informática: Un evento o serie de eventos de seguridad informática no deseados o inesperados, que tienen una probabilidad significativa de comprometer las

[1]Fuente: ISO/IEC 27000:2012

operaciones del negocio y amenazar la seguridad informática. Todo incidente es un evento, más no todo evento es un incidente.[2]

Manual de protección de la información: Documento donde se establecen los lineamientos de seguridad para el manejo de la información del Instituto de Cultura y Patrimonio de Antioquia en función de la clasificación de dicha información. Según la *Política de identificación y protección de la información* la información de la entidad se clasifica en Pública, Clasificada y Reservada.

Plataforma de tecnologías de información / Plataforma de T.I.: Para propósitos del presente documento, las expresiones "plataforma de T.I." y "plataforma de tecnologías de Información" hace referencia a todo el conjunto de recursos de tecnología de la información usados para generar, procesar, almacenar y transmitir información de la Gobernación de Antioquia. Lo que incluye por ejemplo: sistemas de información, equipos de escritorio, portátiles, sistemas operativos, e infraestructura de red.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información:

- Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de mantener la exactitud y estado completo de la información, en otras palabras, proteger la información para que no sea adulterada o alterada de forma indebida.
- Disponibilidad: Propiedad de mantener la información disponible y utilizable cuando lo requiera un individuo, proceso o entidad autorizada.

Seguridad informática: Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

Servidores Públicos: Término que se usa en el presente documento para identificar a empleados públicos, trabajadores oficiales y practicantes del Instituto de Cultura y Patrimonio de Antioquia [3].

Sistema de Gestión de Seguridad de la Información SGSI: Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.

Software malicioso: (También, código malicioso). Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario. El software malicioso incluye virus, gusanos, troyanos, la mayor parte de los rootkits,

[2]Fuente: ISO/IEC 27000:2012
[3] El término "servidor público" está definido en el artículo 123 de la Constitución Política de Colombia.

scareware, spyware, adware intrusivo y crimeware. El término “software malicioso” también hace referencia a software hostil o molesto.

Usuario: Persona, proceso o aplicación de la entidad autorizada para acceder a la información de entidad o a los sistemas que la manejan.

Zonas restringidas de procesamiento: Son áreas, recintos o edificaciones ubicadas dentro de las sedes del Instituto de Cultura y Patrimonio de Antioquia destinadas a alojar Plataformas de tecnología de la información, recursos importantes o información de la entidad; razón por la que requieren controles especiales de seguridad física y control de acceso.

Documentos relacionados

Documentos externos

- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decreto 2693 DE 2012. “Lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia”.
- La Ley 527/1999. “Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Norma Internacional de gestión ISO 27001:2013.

Política general de seguridad informática

La información es un activo estratégico para las operaciones diarias del Instituto de Cultura y Patrimonio de Antioquia y a su vez un factor determinante para el éxito de su plan estratégico. Por ello, la Entidad está comprometida con la adopción de buenas prácticas de seguridad informática tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI.

El Instituto de Cultura y Patrimonio de Antioquia espera el compromiso de todos sus servidores públicos y contratistas con el cumplimiento del presente Manual de Políticas.

1. Políticas para servidores públicos y contratistas

Alcance

Estas políticas aplican tanto a los procesos realizados directamente por el Instituto de Cultura y Patrimonio de Antioquia, como a los ejecutados a través de contratos o acuerdos con terceros.

Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos que hagan uso de la información de la entidad y de sus recursos tecnológicos en las siguientes ubicaciones:

- Instituto de Cultura y Patrimonio de Antioquia.

Las políticas de seguridad informática también aplican para los servidores públicos que llegaran a acogerse en la modalidad de teletrabajo.

1.1 Políticas de identificación y protección de la información

DECLARACIÓN PRINCIPAL:

- Los activos de información dentro del alcance del SGSI del Instituto de Cultura y Patrimonio de Antioquia deben ser identificados, clasificados y definidos los responsables de cada uno de ellos.

1.1.1 Identificación y clasificación de la información

1.1.1.1 Los activos de información deben ser identificados y registrados en un inventario.

1.1.1.2 Los activos de información deben tener propietario designado.

1.1.1.3 El Propietario de un activo de información es responsable de:

- Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
- Determinar las clasificaciones correspondientes a la sensibilidad del activo.
- Asegurar que se gestione el riesgo de seguridad del activo.
- Establecer las reglas de uso del activo, cuando sea necesario.
- Solicitar la aplicación de controles para la protección del activo de información.

1.1.1.4 Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.

- La información del Instituto de Cultura y Patrimonio de Antioquia

1.1.1.5 Se clasifica en:

- **Información pública.** Es toda información que el Instituto de Cultura y Patrimonio de Antioquia genere, obtenga, adquiera, o controle en su calidad de obligado[4].
- **Información clasificada.** Es aquella información que estando en poder o custodia del Instituto de Cultura y Patrimonio de Antioquia en su calidad de obligado, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).
- **Información reservada.** Es aquella información que estando en poder o custodia del Instituto de Cultura y Patrimonio de Antioquia en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

1.1.1.6 El manejo de la información del Instituto de Cultura y Patrimonio de Antioquia debe seguir los lineamientos del Manual de Protección de la Información.

1.1.1.7 Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.

1.1.1.8 El Instituto de Cultura y Patrimonio de Antioquia tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto el Instituto de Cultura y Patrimonio de Antioquia se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información.

1.1.1.9 Los servidores públicos y contratistas son responsables de proteger la información de su trabajo y solicitar a la Dirección de Informática el almacenamiento seguro de la

[4] El término "obligado" se refiere a cualquier persona natural o jurídica, pública, o privada incluida en el artículo 5 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional). Según el literal A del artículo en cuestión, es sujeto obligado: "Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital".

información cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.

1.2 Política de gestión del riesgo de seguridad informática

DECLARACIÓN PRINCIPAL:

En el Instituto de la Cultura y Patrimonio de Antioquia la gestión de los riesgos fundamenta la toma de decisiones de seguridad informática.

1.2.1 Lineamientos generales de la gestión del riesgo de seguridad informática

1.2.1.1 Servidores públicos y contratistas del Instituto de la Cultura y Patrimonio de Antioquia deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

1.3 Política de gestión de incidentes de seguridad informática

DECLARACIÓN PRINCIPAL:

En el Instituto de Cultura y Patrimonio de Antioquia los eventos e incidentes de seguridad informática son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

1.3.1 Reporte de eventos, incidentes y debilidades de la seguridad informática

1.3.1.1 Los servidores públicos y contratistas deben reportar inmediatamente al Centro de Servicios de Informática CSI, todas las situaciones que puedan afectar la seguridad informática.

1.3.1.2 La información específica sobre Incidentes o vulnerabilidades de seguridad informática, así como el detalle de las medidas para proteger las Plataformas de T.I., debe ser tratada como información *Reservada*[5].

[5] Diríjase al manual de protección de la información para consultar las medidas de tratamiento para información *reservada*.

1.4 Política de uso adecuado de los recursos de la plataforma de T.I.

DECLARACIÓN PRINCIPAL:

Toda la información de Instituto del Cultura y Patrimonio de Antioquia, así como los recursos para su procesamiento, almacenamiento y transmisión deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, derroche, uso ilegal o desaprovechamiento.

1.4.1 Requerimientos generales para el uso adecuado de la plataforma de T.I.

1.4.1.1 Se prohíbe el uso de los recursos de plataforma de T.I. del Instituto de Cultura y Patrimonio de Antioquia para la realización de cualquier actividad ilegal.

1.4.1.2 Para verificar el cumplimiento de las presentes políticas; el Instituto de Cultura y Patrimonio de Antioquia podrá monitorear y auditar las Plataformas de T.I. de la entidad que son facilitadas a servidores públicos y contratistas para el cumplimiento de sus deberes y funciones laborales.

1.4.1.3 Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.

1.4.1.4 Está prohibida la realización de pruebas a los controles de seguridad informática.

1.4.1.5 No está permitido aprovechar las vulnerabilidades de seguridad de las plataformas de T.I.

1.4.2 Uso adecuado del correo electrónico

1.4.2.1 No está permitido enviar correos masivos sin la autorización del personal directivo de la dependencia o de las áreas de Talento humano o Comunicaciones.

1.4.2.2 La Dirección de Informática podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.

1.4.3 Uso adecuado de equipos de cómputo asignados

1.4.3.1 No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.

1.4.3.2 Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.

1.4.4 Uso adecuado de servicios de red

1.4.4.1 No deben almacenarse archivos personales en carpetas de la red.

1.4.4.2 No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person). Por ejemplo: Torrent, Ares, eMule, Limewire, GNUnet, entre otros.

1.4.4.3 No está permitida la descarga de archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.

1.4.4.4 No está permitido deshabilitar o evadir los controles de navegación en internet.

1.4.4.5 En horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos.

1.4.4.6 El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.

1.4.4.7 El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público o contratista responsable de dicho equipo.

1.4.4.8 Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público o contratista responsable del equipo de cómputo lo aprueba.

1.4.4.9 Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.

1.4.4.10 La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente el Instituto de Cultura y Patrimonio de Antioquia.

1.4.5 Uso de material protegido por derechos de autor

1.4.5.1 El uso del software que es propiedad del Instituto de Cultura y Patrimonio de Antioquia es para el uso exclusivo de la entidad.

1.4.5.2 Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red de la entidad.

1.4.5.3 Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en la plataforma tecnológica de la entidad.

1.5 Política de personas y cultura frente a la seguridad informática

DECLARACIÓN PRINCIPAL:

Se deben aplicar medidas de control antes, durante y después de finalizada la relación laboral, con el fin de mitigar los riesgos de seguridad informática asociados al factor humano.

1.5.1 Antes del empleo

1.5.1.1 Toda persona a ser contratada como servidor público, debe aceptar formalmente el cumplimiento de las políticas del presente manual.

1.5.2 Durante el empleo o la vigencia del contrato

1.5.2.1 Los servidores públicos y contratistas del Instituto de Cultura y Patrimonio de Antioquia son responsables por desempeñar sus funciones cumpliendo las políticas definidas en el presente manual.

1.5.2.2 Los servidores públicos y contratistas del Instituto de Cultura y Patrimonio de Antioquia son responsables por desempeñar sus funciones sin descuidar, ignorar o desestimar los controles de seguridad establecidos.

1.5.2.3 Los servidores públicos y contratistas que tengan acceso a la información del Instituto de Cultura y Patrimonio de Antioquia deben participar en las actividades o iniciativas de concientización y capacitación en materia de seguridad informática a las que sea convocado.

1.5.2.4 El incumplimiento de las políticas consignadas en el presente manual podrá generar acciones disciplinarias[6].

1.5.2.5 Las políticas de seguridad informática forman parte integral de los contratos de trabajo de los servidores públicos.

1.5.3 Terminación del contrato o cambio de cargo

1.5.3.1 Servidores públicos y contratistas que finalicen su relación laboral con la Entidad deben entregar a su superior inmediato o responsable, la información de la entidad que se encuentre bajo su responsabilidad y/o manejo.

1.5.3.2 La información y el conocimiento desarrollado por los servidores públicos del Instituto de Cultura y Patrimonio de Antioquia durante el horario laboral y dentro de la vigencia del contrato laboral es propiedad de la entidad, por lo tanto se prohíbe el borrado o la copia

[6] Ver cláusula de manejo disciplinario.

de dicha información por parte de servidores públicos y contratistas en proceso de retiro o por personal retirado.

1.5.3.3 Ante la finalización de la relación laboral o contractual de un servidor público o contratista con del Instituto de Cultura y Patrimonio, se deben suspender inmediatamente los permisos de acceso a la plataforma de T.I. de la entidad.

1.5.3.4 La Dirección de Personal debe informar inmediatamente a la Dirección de Informática, los retiros o traslados de los servidores públicos y practicantes, con el fin de revocar o modificar los privilegios de acceso asignados ha dicho personal.

1.5.3.5 El superior inmediato de servidores públicos y contratistas es el responsable de gestionar el retiro o modificación de los derechos de acceso ante novedades laborales como la terminación o cambio del contrato.

1.5.3.6 El superior inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los servidores públicos y contratistas en proceso de retiro.

1.6 Política de seguridad informática para contratación

DECLARACIÓN PRINCIPAL:

La información del Instituto de Cultura y Patrimonio de Antioquia debe ser protegida en los procesos de contratación en todas sus etapas.

1.6.1 Disposiciones generales

1.6.1.1 Se deben designar servidores públicos de la entidad como supervisores de los servicios, funciones y contratos llevados a cabo por terceras partes.

1.6.1.2 Los servidores públicos y contratistas responsables por los servicios de contratistas o proveedores, son responsables de identificar y valorar los riesgos de la información asociados al acceso de éstos.

1.6.1.3 Los contratos celebrados entre el Instituto de Cultura y Patrimonio de Antioquia y contratistas o proveedores con acceso a la información de la entidad, deben incluir cláusulas para mitigar riesgos de seguridad informática.

1.6.1.4 Todos los proponentes invitados a un proceso de negociación o selección (contratistas o proveedores potenciales) deben firmar previamente un acuerdo de confidencialidad, siempre que dicho proceso implique la entrega de información Clasificada o Reservada de la entidad.

1.7 Política de seguridad física de la información y los equipos de cómputo

DECLARACIÓN PRINCIPAL:

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

1.7.1 Seguridad en las instalaciones

1.7.1.1 Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de tal manera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.

1.7.1.2 Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación al personal de vigilancia.

1.7.1.3 Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.

1.7.1.4 Las reuniones y sesiones de videoconferencias del Instituto de Cultura y Patrimonio de Antioquia no deben ser grabadas en audio o video a menos que todos los participantes estén al tanto de la dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.

1.7.1.5 No está permitido fumar, ingerir alimentos o bebidas en las salas con equipos de cómputo.

1.7.2 Seguridad de los equipos

1.7.2.1 Los servidores públicos y contratistas del Instituto de Cultura y Patrimonio de Antioquia son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla (pero sin limitarse a) su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.

1.7.2.2 Los equipos suministrados por el Instituto de Cultura y Patrimonio de Antioquia, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.

1.7.2.3 Se debe bloquear la sesión cuando el usuario se aleje del computador.

1.7.2.4 La salida de los computadores (de escritorio o portátiles) del Instituto de Cultura de Patrimonio de Antioquia debe ser autorizada por el superior inmediato del servidor público

interesado o de quien se haya definido en cada organismo, que pueda ejercer esa función y avalada por la Subsecretaría de Apoyo Logístico.

1.7.2.5 Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al centro de servicios informáticos CSI.

1.7.2.6 El instituto de Cultura y Patrimonio de Antioquia no está obligada a prestar soporte técnico a equipos de cómputo que no sean propiedad de la entidad.

1.7.2.7 Los equipos de cómputo que no sean entregados por el Instituto de Cultura y Patrimonio de Antioquia no deben conectarse a la red de la entidad, a menos que cumplan con los requisitos definidos por el área de Informática.

1.8 Política de control de acceso a plataformas de tecnología de la información

DECLARACIÓN PRINCIPAL:

El Instituto de Cultura y Patrimonio de Antioquia otorga el nivel de acceso necesario a la información y su plataforma de T.I. para el cabal cumplimiento de las funciones de los servidores públicos y contratistas.

1.8.1 Gestión de acceso a usuarios

1.8.1.1 Los dueños de los sistemas de información deben verificar que los privilegios de acceso de los usuarios en las Plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.

1.8.1.2 Los privilegios de acceso otorgados a los usuarios de las Plataformas de tecnología de la información deben ser autorizados por el superior inmediato.

1.8.1.3 Los privilegios de acceso otorgados a los usuarios de las Plataformas de Tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.[7]

1.8.1.4 No están permitidas las cuentas de usuarios genéricas para el ingreso a la Plataforma de T.I.

1.8.1.5 Todas las cuentas de usuario son personales e intransferibles.

1.8.1.6 Servidores públicos y contratistas del Instituto de Cultura y Patrimonio de Antioquia deben reportar a su Jefe cuando tengan más derechos de acceso de los necesarios.

[7] Los dueños de la información se identifican en el inventario de activos de información.

1.8.1.7 A excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica del Instituto de Cultura y Patrimonio de Antioquia, a menos que lo requieran en virtud de sus funciones laborales (como los Administradores de plataforma de T.I. de la entidad).

1.8.1.8 En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un servidor público ausente, el jefe directo respectivo será el único autorizado para solicitar el acceso.

1.8.2 Manejo de contraseñas

1.8.2.1 Los usuarios de las Plataformas de Tecnologías de la Información del Instituto de Cultura y Patrimonio de Antioquia deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.

1.8.2.2 Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.

1.8.2.3 El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.

1.8.2.4 Los usuarios de las Plataformas de T.I. tienen la responsabilidad de cambiar su contraseña (o solicitar su cambio, si es el caso) en el evento que fuese revelada o existiese alguna sospecha de ello.

1.8.2.5 Todos los usuarios de Las Plataformas de Tecnología de Información de la entidad deben emplear contraseñas seguras, es decir, que cumplan las siguientes características:

- 7 Caracteres como mínimo.
- Deben incluir letras mayúsculas y minúsculas.
- Deben incluir números.
- Deben incluir caracteres especiales, por ejemplo !@#$%&*.
- No deben basarse en información personal como: fechas de cumpleaños, direcciones, números telefónicos, nombres de personas, números de documentos de identificación, nombre de la entidad, etc.
- No deben basarse en información de la entidad, es decir, no deben hacer referencia al nombre de la entidad, sus procesos, dependencias, áreas o funciones.

1.9 Política de operación de plataformas de tecnología de información

DECLARACIÓN PRINCIPAL:

El Instituto de Cultura y Patrimonio de Antioquia aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones.

1.9.1 Requisitos para la planeación y operación de las plataformas de T.I.

1.9.1.1 Todas las adquisiciones de software y hardware deben estar avaladas técnicamente por la Dirección de Informática.

1.9.1.2 Los componentes y sistemas de la infraestructura de seguridad informática, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la Dirección de Informática.

1.9.2 Protección contra software malicioso

1.9.2.1 No está permitido el ingreso intencionado de software malicioso a los equipos y redes del Instituto de Cultura y Patrimonio de Antioquia.

1.9.2.2 La presencia identificada o sospechada de software malicioso debe ser reportada al Centro de servicios de Informática CSI.

1.9.3 Intercambio de información

1.9.3.1 Todo intercambio de información con terceras partes debe ser realizado de conformidad a lo dispuesto en el Manual de Protección de la Información.

1.10 Políticas de cifrado de la información

DECLARACIÓN PRINCIPAL:

Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información *clasificada* o *reservada* de la entidad.

1.10.1 Cifrado

1.10.1.1 Servidores públicos y contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al Equipo de Seguridad de la información, novedades acerca del manejo de dichas llaves (por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado).

1.10.1.2 Cada vez que se utilice el cifrado, los servidores públicos y contratistas no deben borrar la única versión legible de los datos, a menos que hayan probado que el proceso de des-cifrado puede restablecer una versión legible de los datos.

1.10.1.3 Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información *reservada* o *clasificada* en medios removibles (como memorias USB, discos duros externos, CD y DVD).

1.10.1.4 Se deben utilizar mecanismos de cifrado cuando se requiera enviar información *reservada* o *clasificada* a través de correo electrónico.

1.11 Política de dispositivos móviles

DECLARACIÓN PRINCIPAL

- El acceso a los datos y sistemas de información del Instituto de Cultura y Patrimonio de Antioquia a través de dispositivos móviles[8] debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad informática.

1.11.1 Computadores portátiles

1.11.1.1 Los usuarios que tengan bajo su responsabilidad computadores portátiles del Instituto de Cultura y Patrimonio de Antioquia son responsables de su protección dentro y fuera de las instalaciones de la entidad.

1.11.1.2 Todo usuario al que se le asigne o facilite un computador portátil del Instituto de Cultura y Patrimonio de Antioquia debe asegurarlo adecuadamente al puesto de trabajo con la guaya de seguridad.

1.11.1.3 Los usuarios de computadores portátiles del Instituto de Cultura y Patrimonio de Antioquia deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad. Las medidas de protección incluyen, pero no se limitan a:

- Llevar los computadores portátiles como equipaje de mano en viajes terrestres y aéreos.
- Mantener a la vista y vigilar el computador portátil en todo momento que se esté fuera de las instalaciones de la entidad o de la vivienda del servidor público.
- Ocultar el computador portátil de la vista de personas externas cuando se esté transportando en un vehículo.
- Utilizar la guaya de seguridad.

1.11.1.4 Los computadores portátiles están cubiertos por la sección “Seguridad física de los equipos” del presente manual de políticas.

[8] Consultar en la sección de definiciones.

1.11.2 Dispositivos móviles diferentes a computadores portátiles

Nota: esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.

1.11.2.1 Los usuarios de dispositivos móviles entregados por el Instituto de Cultura y Patrimonio de Antioquia son responsables de su protección dentro y fuera de las instalaciones de la entidad.

1.11.2.2 Los usuarios de dispositivos móviles entregados por el Instituto de Cultura y Patrimonio de Antioquia deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.

1.11.2.3 Los usuarios de dispositivos móviles entregados por el Instituto de Cultura y Patrimonio de Antioquia deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.

1.11.2.4 No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales (como WhatsApp, LIME o Blackberry BBN PIN).

1.11.2.5 El Instituto de Cultura y Patrimonio de Antioquia no está obligada a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedad de la entidad.

1.11.2.6 Los usuarios que accedan a los servicios de la plataforma de T.I. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo al centro de servicios informáticos CSI.

1.12 Política de cumplimiento

DECLARACIÓN PRINCIPAL:

El instituto de Cultura y Patrimonio de Antioquia cumple la regulación y legislación vigente aplicable en materia de seguridad informática.

1.12.1 Cumplimiento legal y normativo

1.12.1.1 Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilizare registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requerida para una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, área o persona física o jurídica.

1.12.1.2 Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.

1.12.1.3 La realización de auditorías (verificaciones o pruebas de seguridad) no deben afectar la normal operación de los sistemas de información o plataformas.

2. Políticas para el personal de los equipos de trabajo de informática

Alcance

Estas Políticas aplican exclusivamente a personal de los equipos de Informática del Instituto de Cultura y Patrimonio de Antioquia ya sea interno o externo, en el ámbito del proceso de Planeación y Administración de las TIC.

2.1 Política de gestión del riesgo de seguridad informática

DECLARACIÓN PRINCIPAL:

En el Instituto de Cultura y Patrimonio de Antioquia, la gestión de los riesgos fundamenta la toma de decisiones de seguridad informática.

2.1.1 Lineamientos generales de la gestión del riesgo de seguridad informática

2.1.1.1 Se deben identificar los riesgos a los que se encuentran expuestos los activos de información de la entidad.

2.1.1.2 Los criterios de evaluación y aceptación de riesgos de seguridad informática deben estar alineados con los criterios y políticas de gestión del riesgo de la entidad.

2.1.1.3 Los riesgos de seguridad informática analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.

2.1.1.4 Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.

2.1.1.5 En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos.

2.2 Política de gestión de incidentes de seguridad informática

DECLARACIÓN PRINCIPAL:

En el Instituto de Cultura y Patrimonio de Antioquia los eventos e incidentes de seguridad informática son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

2.2.1 Gestión de los Incidentes de seguridad informática

2.2.1.1 Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamiento a los incidentes de seguridad informática.

2.2.1.2 La atención de incidentes debe seguir los procedimientos de Atención de Acciones preventivas o Atención de acciones Correctivas.

2.3 Política de seguridad informática asociada a contratistas

DECLARACIÓN PRINCIPAL:

La información del Instituto de Cultura y Patrimonio de Antioquia debe ser protegida de los riesgos generados por el manejo o acceso de contratistas y proveedores.

2.3.1 Requisitos de seguridad informática asociados a contratistas y terceros

2.3.1.1 El acceso de contratistas y proveedores a información o a plataformas de tecnología de Información del Instituto de Cultura y Patrimonio de Antioquia, se concede solamente cuando se demuestre la necesidad de su uso y esté expresamente autorizado por el propietario del activos de información o sistema de información respectivo.

2.3.1.2 Únicamente debe concederse acceso remoto a plataformas de tecnología de Información a contratistas y proveedores, cuando estos tengan una necesidad legítima que lo justifique. El acceso remoto debe limitarse al tiempo requerido para cumplir con las actividades, debe ser autorizado por el propietario del activo respectivo, y posteriormente gestionado por personal autorizado de la Dirección de Informática.

2.3.1.3 El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (logs de auditoría) de dichas labores.

2.4 Seguridad física de la información y los equipos de cómputo

DECLARACIÓN PRINCIPAL:

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

2.4.1 Zonas restringidas de procesamiento

2.4.1.1 Se deben identificar y especificar las zonas restringidas de procesamiento del Instituto de Cultura y Patrimonio de Antioquia destinadas a alojar equipos y dispositivos de la plataforma de T.I. de la entidad.

2.4.1.2 Cada zona restringida de procesamiento debe tener un responsable.

2.4.1.3 Las zonas restringidas de procesamiento deben contar al menos con mecanismos de control de acceso y vigilancia.

2.4.1.4 Se deben definir las reglas para el trabajo al interior de las zonas restringidas de procesamiento, dichas reglas deben ser documentadas y publicadas en un lugar visible de cada una de estas zonas.

2.4.1.5 Todo sistema, equipo, dispositivo, o medio crítico para la transmisión, procesamiento y almacenamiento de la información del Instituto de Cultura y Patrimonio de Antioquia debe ser ubicado dentro de zonas restringidas de procesamiento. Si no se pudiera ubicar algún equipo dentro de estas zonas, dicho equipo debe ser objeto de controles complementarios de acceso físico.

2.4.1.6 Sólo personal autorizado por el responsable de cada zona restringida de procesamiento puede ingresar a dicha zona.

2.4.1.7 Se debe generar y mantener registro de los accesos de personal externo a las zonas restringidas de procesamiento que contengan infraestructura crítica de TI. El periodo de retención para estos registros es de tres meses como mínimo.

2.4.1.8 En el caso particular del centro de cómputo, se debe generar y mantener registro de los accesos de personal tanto interno como externo. El periodo de retención para estos registros es de tres meses como mínimo.

2.4.1.9 El personal no autorizado interno o externo sin acompañamiento dentro de las zonas restringidas de procesamiento debe ser retirado de dicho lugar y además debe notificarse al responsable de la zona restringida de procesamiento respectiva.

2.4.1.10 Los privilegios de acceso a las zonas restringidas de procesamiento deben ser revisados al menos cada trimestre.

2.4.1.11 Las zonas restringidas de procesamiento deben estar dispuestas para brindar condiciones ambientales adecuadas (como temperatura y humedad) para mantener de forma óptima los recursos y la información allí alojados.

2.4.2 Seguridad física de los equipos

2.4.2.1 Siempre que se reutilice un servidor, computador portátil o un computador de estación de trabajo, se requiere la realización previa de un Borrado Seguro de la información almacenada en dichos equipos antes que sean entregados a los nuevos usuarios.

2.4.2.2 Debe realizarse Borrado Seguro de los equipos de forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción).

2.4.2.3 Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados por amenazas del entorno (es decir, evitando daños derivados de situaciones como manifestaciones sociales, inundaciones, humedad o incendio).

2.4.2.4 Todos los equipos de procesamiento críticos deben tener controles para evitar caídas de la plataforma de TI causadas por fallas en el servicio eléctrico.

2.5 Control de acceso a plataformas de tecnología de la información

DECLARACIÓN PRINCIPAL:

El Instituto de Cultura y Patrimonio de Antioquia otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones.

2.5.1 Proceso de control de acceso

2.5.1.1 El control de acceso es una característica indispensable para las plataformas de tecnología de la información del Instituto de Cultura y Patrimonio de Antioquia.

2.5.1.2 Todo proceso de control de acceso debe tener un responsable de su gestión.

2.5.1.3 La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.

2.5.1.4 Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad informática.

2.5.1.5 El acceso remoto a plataformas de tecnología de la información del Instituto de Cultura y Patrimonio de Antioquia debe ser autorizado por los dueños de las plataformas respectivas.

2.5.1.6 El acceso remoto a plataformas de tecnología de la información del Instituto de Cultura y Patrimonio de Antioquia debe ser realizado a través de VPN u otros medios que garanticen la seguridad en la comunicación.

2.5.2 Gestión de acceso a usuarios

2.5.2.1 Las cuentas de administración de las Plataformas de tecnología de la información sólo deben ser usadas cuando sea necesario dicho privilegio.

2.5.3 Manejo de contraseñas

2.5.3.1 Los nombres de usuario y contraseñas se rigen por el Criterio de seguridad informática del Instituto de Cultura y Patrimonio de Antioquia.

2.5.3.2 Las contraseñas de administración de las Plataformas de tecnología de la información del Instituto de la Cultura y Patrimonio de Antioquia podrán ser escritas en medios físicos o electrónicos únicamente si son objeto de medidas de seguridad física y/o lógica, según lo establecido en el Criterio de seguridad informática del Instituto de Cultura y Patrimonio de Antioquia.

2.6 Operación de tecnologías de información y comunicaciones

DECLARACIÓN PRINCIPAL:

El Instituto de Cultura y Patrimonio de Antioquia aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones.

2.6.1 Requisitos para la planeación y operación de las Plataformas de tecnología de la información

2.6.1.1 Las nuevas plataformas o soluciones de tecnologías de la información del Instituto de la Cultura y Patrimonio de Antioquia deben ser analizadas en la fase de planificación con el fin de identificar los requisitos funcionales y de seguridad informática.

2.6.1.2 Las Plataformas Tecnológicas de la Entidad deben ser configuradas de conformidad con el Criterio de seguridad informática del.

2.6.1.3 La realización de auditorías, verificaciones o pruebas de seguridad informática no deben afectar la normal operación de las Plataformas de tecnología de la información.

2.6.2 Protección contra software malicioso y móvil

2.6.2.1 La plataforma de T.I del Instituto de Cultura y Patrimonio de Antioquia debe ser objeto de protección frente software malicioso.

2.6.3 Respaldo de la información

2.6.3.1 La información importante de la entidad alojada en los repositorios de red y los sistemas de información críticos deben ser respaldados a intervalos programados.

2.6.3.2 Los respaldos de información deben ser probados regularmente, para verificar que la información si es recuperable ante un incidente.

2.6.3.3 Los respaldos de información deben almacenarse además en un lugar externo al Instituto de la Cultura y Patrimonio de Antioquia, evitando que ante la posibilidad de un desastre al interior de la misma, se pierda por completo la información.

2.6.4 Intercambio de información

2.6.4.1 Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información clasificada.

2.6.4.2 La creación de una conexión directa entre las Plataformas de tecnología de la información del Instituto de la Cultura y Patrimonio de Antioquia y las organizaciones externas a través de Internet o cualquier otra red pública, debe estar autorizada por el Área de sistemas.

2.7 Adquisición, desarrollo y mantenimiento de sistemas de información

DECLARACIÓN PRINCIPAL:

Los aplicativos del Instituto de Cultura y Patrimonio de Antioquia deben ser asegurados en sus fases de planeación, adquisición, desarrollo, implementación y operación.

2.7.1 Requerimientos de seguridad de los sistemas de información

2.7.1.1 Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.

2.7.1.2 Los requisitos de seguridad de los aplicativos deben incorporar los lineamientos del Criterio de seguridad informática del Instituto de la Cultura y Patrimonio de Antioquia aplicables o aquellos que sean definidos por la Subdirección Administrativa y financiera.

2.7.1.3 La contratación de un desarrollo a medida, adquisición de software o sistemas de información debe incluir entrenamiento en administración de las funciones de seguridad de dichas aplicaciones.

2.7.1.4 La contratación de un desarrollo a medida, adquisición o modificación de software o sistemas de información debe incluir la entrega de la documentación y la transferencia de conocimiento técnico y operativo suficiente al personal de soporte del Instituto de Cultura y Patrimonio de Antioquia.

2.7.1.5 Deben definirse requisitos previos a la contratación de proveedores de desarrollo o soporte de software y sistemas de información que incluyan:

- Aseguramiento de la disponibilidad y continuidad del servicio.
- Condiciones para la entrega de código fuente al Instituto de Cultura y Patrimonio de Antioquia (por ejemplo: ante el incumplimiento del proveedor) cuando el código fuente no sea propiedad de la entidad.
- Acuerdos de niveles de servicio (ANS) adecuados a la criticidad de la aplicación desarrollada o soportada por el proveedor.
- Requisitos de seguridad, al menos los listados en el instructivo "Requisitos de seguridad para desarrollo de aplicaciones Web", en el caso desarrollo de aplicativos web.
- La realización de verificaciones de la seguridad a la aplicación; ya sean estas auditorías al código fuente o pruebas de seguridad.

2.7.2 Gestión de vulnerabilidades técnicas

2.7.2.1 Se debe verificar que el procesamiento del aplicativo es correcto, tanto en ambiente de pruebas como de producción, así como el cumplimiento de los requisitos definidos en la etapa de planeación

2.7.2.2 Las vulnerabilidades técnicas de las Plataformas de tecnología de la información deben ser objeto de un procedimiento de gestión orientado a la remediación de dichas vulnerabilidades.

2.7.3 Cifrado

2.7.3.1 Los controles de cifrado empleados en la entidad deben seguir los requerimientos del Criterio de Seguridad Informática del Instituto de Cultura y Patrimonio de Antioquia.

2.7.3.2 Las llaves criptográficas deben tener un custodio designado.

2.7.3.3 Se debe mantener un inventario de las llaves criptográficas que son responsabilidad de informática.

2.7.4 Seguridad de los archivos del sistema

2.7.4.1 El personal de desarrollo de sistemas de información no debe tener facultad para trasladar o modificar software al ambiente de pruebas ni al ambiente de producción.

2.7.4.2 A menos que se obtenga un permiso por escrito del propietario de la información (dueño de las bases de datos) toda prueba a sistemas de información (o a funcionalidades de estos) diseñados para manejar información reservada o clasificada:

- Debe llevarse a cabo con datos que no sean clasificados o reservados, o;
- Deben emplearse soluciones de ofuscación datos, que impidan la correlación de la información por parte de eventuales atacantes.

2.7.4.3 Sólo el personal responsable del desarrollo de software debe tener acceso al código fuente.

2.8 Dispositivos móviles

DECLARACIÓN PRINCIPAL:

El acceso a los datos y sistemas de información del Instituto de Cultura y Patrimonio de Antioquia a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad informática.

2.8.1 Computadores portátiles

2.8.1.1 Los computadores portátiles de la entidad deben tener instalada una herramienta de cifrado de datos que impida la fuga de información en caso de robo, pérdida o intentos de acceso no autorizado al equipo.

3. Políticas de Backups

Alcance

Estas Políticas aplican exclusivamente a los procesos de bases de datos, imágenes y otras informaciones que se procesan en los servidores para el óptimo desempeño de los aplicativos, los cuales debemos custodiar y proteger en el Instituto de Cultura y Patrimonio de Antioquia tanto a nivel interno como externo, en el ámbito de Planeación y Administración de las TIC.

3.1 Backups

DECLARACIÓN PRINCIPAL:

El acceso a los datos y sistemas de información del Instituto de Cultura y Patrimonio de Antioquia garantizan la estabilidad en nuestros procesos a diario, pero estos deben estar respaldados para posibles desastres informáticos el cual se realiza de forma y controlada con el fin de evitar incidentes de seguridad y perdida de la información.

3.1.1 Bases de datos.

Este proceso de backup se genera desde varios motores de bases de datos, en el servidor de ORACLE allí reside un comando que realiza un backup full cada 6 horas y elimina el anterior u obsoleto, lo cual ayuda a minimizar el consumo de alojamiento y mantiene este proceso actualizado, este se realiza para las bases de datos de SICOF por ahora, para DOCUWARE desde este propio server y a nivel se SQL SERVER se realiza un backup dos veces al día programado a las 12pm y a las 6m, KOHA maneja un backup diario q se realiza una vez al día 12pm, los aplicativos SICPA los respalda el contratista hasta ser migrados a nuestro servidor.

Este backup se genera también a un disco externo como primera medida de contingencia y queda a nivel interno del instituto y también se genera a otro disco externo por fuera del instituto como segunda medida de contingencia en caso de un desastre tecnológico o de seguridad informática.

3.1.2 Backups de imágenes

El backup de imágenes se comenzó a generar desde la implementación tecnológica de gestión documental (DOCUWARE), estas imágenes digitalizadas reposan en una unidad de almacenamiento que cuenta con un tamaño de 600gg y que es modificable según el crecimiento, se encuentra en un raid nivel 5 a nivel de Linux conocido como FILESERVER.

Este backup se genera también a un disco externo como primera medida de contingencia y queda a nivel interno del instituto y también se genera a otro disco externo por fuera del instituto como segunda medida de contingencia en caso de un desastre tecnológico o de seguridad informática.

3.1.3 Backup externos.

Los backups externos se utilizan como segunda medida de contingencia y se realizan desde el instituto a esta unidad por fuera de este, de manera periódica una vez al día, todos los procesos de backup descriptos en este punto 3 se hacen de manera completa pero diferencial por tamaño y fecha.

Listado de anexos

Manual de Protección de la Información

ELABORO	REVISO	APROBO
Raúl Augusto Restrepo Granada Técnico Administrativo (TICS) Fecha: 19/01/015	Maribel Sandoval Hernández Gabriel Hernandez Fecha: 00/00/2015	Jairo Alonso Escobar Velasquez Fecha: 00/00/2015