INSTITUTO POPULAR DE CULTURA
Alcaldía de Santiago de Cali

SEGURIDAD DE LA INFORMACION

POLITICA PARA LA SEGURIDAD DE LA INFORMACION
INSTITUTO POPULAR DE CULTURA

PRESENTADO POR:

STEVENS SANDOVAL SANDOVAL
COORDINADOR DE TELEMATICA

TABLA DE CONTENIDO

Contenido

1. INTRODUCCION

La Información que día a día producen las instituciones públicas, se han convertido en uno de los activos más valiosos para el funcionamiento a poste ori, es por eso, que tener una política que establezca los lineamientos para la protección de la información, se convierte en un paso adelantado hacia la transformación tecnológica la cual estamos viviendo.

Ir un paso a delante nos permitirá establecer un control organizado de los procesos informáticos que se han establecido como aliados al desarrollo funcional de las instituciones. La efectividad en la administración y protección de los datos disminuyen los riesgos a perdidas y vulnerabilidades los cuales estamos expuestos al uso de las nuevas tecnologías y del internet de las cosas

2. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información prima en el conjunto de medidas preventivas y reactivas de las organizaciones orientadas a resguardar y proteger la información, la confidencialidad y la disponibilidad e integridad de datos.

Confidencialidad: La información debe ser accesible sólo a aquellas personas autorizadas.

Integridad: El contenido de la información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Disponibilidad: La información sólo pueden ser obtenida a corto plazo por los usuarios que tengan los permisos adecuados para ello.

3. OBJETIVOS

3.1 Proteger, conservar y administrar objetivamente la información del Instituto Popular de Cultura junto con las tecnologías utilizada para su procesamiento. Frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

3.2 Definir las directrices del Instituto Popular de Cultura para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Generalidades

La información digital es hoy en día uno de los recursos más importantes dentro de la institución y por consiguiente debe ser debidamente protegida.

El desarrollo y la aplicación de esta Política garantiza una disminución de los riesgos asociados de daño de la información y se asegura el eficiente cumplimiento de las funciones principales de la entidad apoyadas en un correcto sistema de información.

4.2 Alcance

Esta política es de aplicación en el conjunto de áreas y dependencias que componen la institución, a la totalidad de los procesos internos, a todo el personal del Instituto Popular de Cultura, sin restricción de su situación contractual, el área a la cual se encuentre vinculado y el nivel de las tareas que desempeñe.

4.3 Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Instituto Popular de Cultura, o cualquiera que sea su situación contractual, el área en el cual se encuentre asignado y al nivel de las tareas que desempeñe dentro de la institución.

Las directivas institucionales aprueban esta Política y son responsables de la autorización de sus modificaciones.

El coordinador Administrativo o quien haga sus veces, se encargará de cumplir la función de notificar a todo el personal que se vincula contractualmente con la institución, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Área de Informática Educativa. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de confidencialidad y de tareas de capacitación continua en materia de seguridad.

5. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal del Instituto Popular de Cultura cualquiera sea su situación contractual, la dependencia a la cual pertenezca y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Oficina de Informática y Telemática debe mantener un directorio completo y actualizado de tales perfiles.

La responsabilidad de custodia de cualquier archivo, usado o producido por el personal que se retira, o cambia de cargo, recae en el superior inmediato o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

6. RESPONSABILIDADES DEL PERSONAL DE LA ENTIDAD.

Todo el personal del Instituto Popular de Cultura, cualquiera sea su situación contractual, la dependencia a la cual pertenezca y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

El Estatuto General y el Estatuto Docente deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

(Revisar Jurídicamente este tema)

El área de Informática se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

7. RESPONSABILIDADES DE LOS ESTUDIANTES.

Para poder usar los recursos de TI de la Institución, los estudiantes deben leer y aceptar en cada matrícula de semestre un acuerdo con los términos y condiciones. El área de Informática de Educativa debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

El estatuto estudiantil debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

(Revisar Jurídicamente este tema)

8. RESPONSABILIDADES DE USUARIOS EXTERNOS

Todos los usuarios externos deben estar autorizados por un miembro del personal de la Entidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales.

8.1 no se proporcionara el servicio solicitado por un usuario, o área de trabajo, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

9. USUARIOS INVITADOS Y SERVICIOS DE ACCESO PÚBLICO.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

10. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 ACESO

Se debe tener acceso controlado y restringido a los cuartos de servidores principales y área de comunicaciones. El Área de Informática Educativa elaborara y mantendrán las normas, controles y registros de acceso a dichas áreas.

9.2 SEGURIDAD EN LOS EQUIPOS

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro y protegido con los siguientes parámetros:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.

- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en los servidores del área de Informática Educativa del IPC.

El área de Informática Educativa del IPC define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del área TI IPC.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Es responsabilidad del usuario, cerrar los inicios de sección del respectivo equipo y apagar la estación de trabajo cuando haya terminado su jornada laboral, las estaciones de trabajo no deben quedar encendidos por más de un día.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el área de Informática y Telemática.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

11. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

11.1 REPORTE E INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD

Los Funcionarios del Instituto Popular de Cultura deben reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su Supervisor de área, a la oficina de Informática y Telemática. Estos reportes deben ser llegados a través de medio electrónico, email, o medio físico.

Se debe de establecer comunicado de la alta dirección.

La oficina de Informática Educativa debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

12. PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos. El área de Informática Educativa elaborará y mantendrá un conjunto de normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo del Instituto Popular de Cultura deben estar protegidas por software antivirus con capacidad de actualización en cuanto a firmas de virus y malware maliciosos. Los usuarios de la estación no están autorizados a deshabilitar este control.

El Instituto Popular de Cultura a través del área de Informática podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La oficina de Informática debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

13. COPIAS DE SEGURIDAD

Toda información considerada información institucional de carácter sensible 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 del área de Informática. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

El área de Informática del Instituto debe 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. La Oficina de Informática 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.

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados por la Oficina de Informática Educativa.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo supervisor de área las copias de seguridad para su registro y custodia.

14. ADMINISTRACIÓN DE CONFIGURACIONES DE RED

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad mantenida por la Oficina de Informática Educativa.

Todo equipo de Informática debe ser revisado, registrado y aprobado por la Oficina de Informática Educativa. Antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

15. INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Dirección Administrativa, y dirigida por dichos entes a los responsables de su custodia.

16. INTERNET Y CORREO ELECTRÓNICO

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

El servicio de correo electrónico es exclusivo del IPC y por ende se debe hacer uso de él, en todo lo relacionado con las actividades y funciones diarias de la

institución, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o distribución de software malicioso o mal intencionado. El correo electrónico es de uso exclusivo de los empleados y funcionarios del instituto, por ende el usuario será responsable de la información que sea enviada o eliminada desde su cuenta.

El uso indebido del correo electrónico, será motivo para realizar la suspensión temporal de la cuenta, o en caso contrario y de evidenciarse un posible riesgo para las demás cuentas o infraestructura tecnológica de la institución, se eliminara la cuenta. El administrador de la red corporativa se reserva el derecho de monitorear las cuentas de los diferentes usuarios que presenten un comportamiento sospechoso para la seguridad de la infraestructura tecnológica.

17. INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre equipos de informática de la Institución deben ser aprobadas la Oficina de Informática, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias. El Comité de Informática y Telecomunicaciones definirá el ámbito en el cual actuará cada dependencia.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La Oficina de Informática debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la Oficina de Informática mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

18. CONTROL DE ACCESO

18.1 CATEGORÍAS DE ACCESO

Los accesos a los recursos de tecnologías de información institucionales deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

18.2 CONTROL DE CLAVES Y NOMBRES DE USUARIO

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Corresponde a la Oficina de Informática elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal, estudiantes, docentes y terceros.

La Oficina de Informática debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas, las claves de acceso no deben de ser divulgadas, además los diferentes usuarios no deben obtener por ningún mecanismo las claves de acceso de otros usuarios ya que se considera un acceso indebido y una violación a la seguridad. Las claves de acceso al sistema son asignadas por el mismo usuario y es responsabilidad del mismo mantenerla a salvo.

El Instituto Popular de Cultura debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, los estudiantes, docentes y terceros deben poseer para acceder a los servicios de red.

El control de las contraseñas de red y uso de equipos es responsabilidad de la Oficina de Informática. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por la dirección del área de Informática, y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La Oficina de Informática debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Como requisito para la terminación de relación contractual o laboral del personal de la Institución, la Oficina de Informática debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la institución.

19. CUMPLIMIENTO

Todo uso y seguimiento de uso a los recursos de TI en el Instituto Popular de Cultura debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia, incluido, pero no restringido a:

Constitución Política de Colombia
Ley 5271999 Ley de comercio electrónico.
NTC 27001:2006. Sistema de Gestión de Seguridad de la Información.
ISO/IEC 17799:2005 Information technology Security techniques Code of practice for information security management
Estatuto Docente del Instituto Popular de Cultura
NTCGP1000:2004 Norma Técnica Colombiana de la Gestión Publica

20. REFERENCIAS

[1] ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos.

[2] 1998. Lineamientos para la Gestión de Seguridad TI

[3] ISO/IEC TR 18044:2004. Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información .

[4] NIST SP 80030. Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.

[5] SGIS 2014. Política de Seguridad de la Información-Universidad Distrital