POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN-CASA DE LA CULTURA PIEDRA DEL SOL.

Versión 1
2019

DE CONTENIDO

1. INTRODUCCIÓN

En septiembre 12 de 2019, se establece la Política de Seguridad de la Información de la Casa de Cultura Piedra del Sol de Floridablanca, en donde se establece como medida puntual para mitigar el riesgo de corrupción, la Aplicación política de administración de la información, definida en las siguientes acciones:

1. Adoptar Política de seguridad de la información

2. Conformar Comité de Seguridad de la Información

3. Desarrollar controles de la Política de Seguridad de la Información.

Lo anterior enmarcado además en los esfuerzos que la Casa de cultura Piedra del Sol enfoca en impulsar las Tecnologías de la Información y las Comunicaciones, para garantizar una entidad con mayor y mejor interacción con la ciudadanía a través del uso adecuado de los recursos a su alcance. Es así como la Política de Seguridad de la Información permite avanzar en la estrategia de Gobierno Digital, específicamente en las metas dadas para el componente 1. Elementos Transversales, en conformidad a lo consignado en el Manual para la Implementación de Gobierno Digital, Entidades del Orden Nacional 2012-2015 y de Orden Territorial 2012 -2017, así:

En este componente también se describen actividades orientadas a que cada entidad cuente con una política de seguridad que es aplicada de forma transversal y mejorada constantemente; y que se garantice la incorporación del Gobierno digital como parte de la cultura organizacional y elemento de soporte en sus actividades misionales. Para alcanzar los objetivos de este componente, las entidades deberán desarrollar las siguientes actividades: 1. Institucionalizar la Estrategia de Gobierno Digital; 2. Centrar la atención en el usuario; 3. Implementar un sistema de gestión de Tecnologías de Información;

4. Implementar un sistema de gestión de seguridad de la información (SGSI).
Dentro de los aspectos clave a tener en cuenta para la implementación del SGSI encontramos:

Fundamentales

- Compromiso y apoyo de la Dirección de la Casa de Cultura Piedra del Sol
- Definición clara de un alcance apropiado.
- Concientización y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a los procesos de la Casa de Cultura Piedra del Sol
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Inclusión de la cláusula o dominio gestión de incidentes de seguridad.

Riesgos

- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.

- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de la organización.
- Planes de formación y concientización inadecuados.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concientización y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.
- A continuación, se establecen las políticas sobre las cuales se debe direccionar el desarrollo futuro del Sistema de Gestión de Seguridad de la Información de la Casa de Cultura Piedra del Sol, así como los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información.

Factores críticos de éxito

- La concientización del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y de la organización.

A continuación, se establecen las políticas sobre las cuales se debe direccionar el desarrollo futuro del Sistema de Gestión de Seguridad de la Información de la Casa de Cultura Piedra del Sol, así como los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información.

1.1. ALCANCE

Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos y físicos, que representa los objetivos sobre los que se sustenta el Sistema de Gestión de Seguridad de la Información.

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

El enunciado y la definición de estos lineamientos, comprende todos los aspectos administrativos y de control que deben ser acatados por el Comité de Seguridad de la Información b y los grupos técnicos responsables de la Seguridad de la Información, conformados por dicho Comité, así como el resto de personal que labora para este organismo, con el fin de lograr un adecuado nivel de confidencialidad, integridad, disponibilidad y fácil auditoría de los accesos a la información.

La política de seguridad es de obligatorio cumplimiento para todos los servidores públicos y particulares que accedan a la información de la administración municipal, así como a los espacios físicos del mismo que conlleven un componente de seguridad de información.

Las aplicaciones de las políticas propuestas en este documento obedecen al interés por parte de la Casa de Cultura Piedra del Sol en diseñar, implementar y sostener el Sistema de Gestión de la Seguridad de la Información –SGSI-, el cual deberá tener en cuenta y estar alineado con un Sistema Integrado de Gestión, en cada uno de sus componentes: Sistemas de Gestión de Calidad, Control Interno, Desarrollo Administrativo y Gestión Ambiental.

2. DEFINICIONES.

2.1. Seguridad de la Información

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 a tener acceso a la misma.
• 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 relacionados con la misma, toda vez que lo requieran.
Adicionalmente, deberán considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución.
Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

• **Audibilidad:** 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 La Casa d Cultura Piedra del Sol.
• **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.
A los efectos de una correcta interpretación de la presente Política, 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 por La Casa de Cultura Piedra del Sol o por un tercero que procese información en su nombre, para llevar a cabo una función propia de La Casa de Cultura Piedra del Sol, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2. 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 de La Casa de Cultura piedra del Sol

2.3. 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.

2.4. Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas de La Casa de Cultura piedra del Sol
, destinado a garantizar el apoyo de la gerencia a las iniciativas de seguridad.

2.5. 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 de La Casa de Cultura piedra del Sol que así lo requieran, profesional con experiencia en seguridad informática adscrito a la Secretaría General.

2.6. 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.

2.7. 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.

3. POLITICAS DE SEGURIDAD PARA LA CASA DE CULTURA PIEDRA DEL SOL.

La Casa de Cultura Piedra del Sol, define sus políticas de seguridad con fundamentada en los dominios de controles señalados en la norma NTC/IEC ISO 27001 - NTC/IEC ISO 27002 y que se transcriben a continuación.

3.1. Política de seguridad.

Controles para proporcionar directivas y consejos de gestión para mejorar la Seguridad de la Información Preservar la Seguridad de la Información del organismo, para lo cual dispondrá de los recursos necesarios para garantizar el correcto desarrollo de los lineamientos planteados en cada política propuesta.

3.2. Organización de la Seguridad

Controles para facilitar la gestión de la seguridad de la información en el seno de la organización. Garantizar que existan responsabilidades claramente asignadas en todos los niveles de la organización, para la gestión de la Seguridad de la Información y contar con un Comité de Seguridad de la Información conformado por personal de alto nivel de cada dependencia que se apoyará en un asesor interno de seguridad designado por la Dirección General. Todos los servidores públicos, contratistas y particulares que tengan acceso a los activos de información del organismo, tendrán el compromiso de cumplir las políticas y normas que se dicten en materia de seguridad de la información así, como reportar los incidentes que detecten.

Con el objetivo de direccionar y hacer cumplir los lineamientos del organismo en cada materia y revisar las posibles incidencias y acciones que se deban tomar; tanto el Comité de Seguridad de la Información y el Asesor Interno de Seguridad de la Información, designado por la Dirección General, podrán apoyarse con recursos externos, mejores prácticas, etc.

3.3. Gestión de Activos.

Controles para catalogar los activos y protegerlos eficazmente. Toda la información sensible de la Casa de Cultura Piedra del Sol, así como los activos donde esta se almacena o procesa, deberán ser inventariados, asignárseles un responsable y clasificarlos de acuerdo con los requerimientos en materia de seguridad de la información y los criterios que dicte el Comité de Seguridad de la Información del organismo, de acuerdo con esta clasificación se deben establecer los niveles de protección orientados a determinar, a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación deberá revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.

La Dirección General a través de la Oficina de Sistemas debe brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen

3.4. Seguridad de los Recursos Humanos.

Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos. Desde la vinculación del personal a la Casa de Cultura Piedra del Sol, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo deberán establecer la responsabilidad de los servidores públicos y contratistas, por la Seguridad de la Información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad que se hace extensivo a los contratistas y terceros que tengan acceso a la información.

Deberán existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los servidores públicos deben cooperar con los esfuerzos por proteger la **INFORMACIÓN** y ser responsables de actualizarse en cada materia, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deberá llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.
Para el caso de los contratistas de prestación de servicios o apoyo a la gestión administrativa la responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el supervisor del contrato y para el personal de planta el jefe inmediato; 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.

3.5. Seguridad Física.

Controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos industriales. Deberán establecerse áreas seguras para la gestión, almacenamiento y procesamiento de información en la Casa de Cultura Piedra del Sol, estas deberán contar con protecciones físicas y ambientales acordes a los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados que preserven el medio ambiente.

Esta seguridad debe mantenerse en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir del organismo o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.

ser mantenida en servidores aprobados por La Secretaría General a través de la Oficina de Sistemas. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.
Los Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La Dirección General a través de la Oficina de Sistemas debe asegurar que la infraestructura de servicios de TI esté cubierta por mantenimiento y soporte adecuados de hardware y software.
Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la Administración Municipal de Soacha 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.
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 **Comité de Seguridad en la Información.**

3.6. Gestión de las Telecomunicaciones y Operaciones.

Controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información. Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse. Debe buscarse una adecuada segregación de funciones.

Debe garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura.

Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la red, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.

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

La Dirección General a través de la Oficina de Sistemas podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La Dirección General a través de la Oficina de Sistemas deben 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.

Toda información que pertenezca al inventario de activos de información de la Casa de Cultura Piedra del Sol 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 por el **Comité de Seguridad de la Información**. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

La Dirección General a través de la Oficina de Sistemas debe garantizar la ejecución de las copias de seguridad automatizando el procedimiento por medio de herramientas software de acuerdo a los procedimientos documentados por el **Comité de Seguridad de la Información**.

La Dirección General a través de la Oficina de Sistemas 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 Dirección General a través de la Oficina de Sistemas debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad.

La Oficina Asesora de Control Interno deberá 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. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

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 y mantenida por la La Dirección General a través de la Oficina de Sistemas.

Todo equipo de TI debe ser revisado, registrado y aprobado por La Dirección General a través de la Oficina de Sistemas antes de conectarse a cualquier nodo de la Red de comunicaciones y datos de la Casa de Cultura. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

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 vigente y el manejo responsable de los recursos de tecnologías de la información.

La Dirección General a través de la Oficina de Sistemas a por medio del líder de seguridad informática administrará las herramientas necesarias para filtrar el contenido de internet y creará perfiles para su correcto uso.

El sistema de correo electrónico institucional de la Casa de Cultura Piedra del Sol debe ser usado únicamente para propósitos laborales.

Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos; injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Casa de Cultura Piedra del Sol.

El servicio de correo electrónico de la Institución no debe ser utilizado para enviar correo basura (Spam).
Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar los lineamientos y recomendaciones para dicho tipo de documentos, tales como:

- Iniciar su correo con un saludo formal. Ejemplo: Buenos días Adriana. Cordial saludo.
- Nombrar al destinatario de correo por su nombre o profesión.
- Evitar tutear.
- Evitar el uso de palabras que puedan resultar ofensivas.
- Escribir puntualmente. No extenderse demasiado.
- Al final del correo agradecer por la atención prestada y firmar con los requerimientos establecidos para la firma electrónica institucional (ver al final).

Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes.

Cualquier información de carácter institucional debe ser enviada a través de una cuenta institucional, correos personales no serán tenidos en cuenta

La difusión masiva de comunicaciones debe estar aprobada por el Señor Dirección General, Jefes de Oficina o Directora de Recursos Humanos.
Cualquier información de carácter institucional debe ser enviada a través de una cuenta institucional.

La Casa de Cultura Piedra del Sol debe garantizar que todo el personal que labora en la alcaldía tenga configurada una cuenta de correo institucional.
Los correos electrónicos institucionales deben estar escritos en la fuente Calibri, tamaño 12.

El texto debe estar escrito únicamente en color negro.

No se debe escribir en mayúsculas, ya que puede ser interpretado como un grito u ofensa.
Los correos enviados no deben tener ningún color o imagen sobre el fondo en el que se escribe el mensaje.
La firma de correo debe tener la siguiente estructura:

Cordialmente,
Pepito Pérez | **Secretario Dirección** | Casa de Cultura Piedra del Sol
Tel: +57 (6) 6188181
Dirección vía antigua junto al jardín botánico - Floridablanca, Colombia.
http://www.casadeculturpiedradelsolgov.co | contactenos@casadeculturapiedradelsol.gov.co

Para la firma de los contratistas, es importante señalar el Número de Contrato correspondiente conforme el modelo ilustrativo:
Cordialmente,
Rosa Pérez | Asesor Jurídico No. 564 de 2019| CASA DE CULTURA PIEDRA DEL SOL
Tel: +57 (6) 6188181
Dirección vía antigua junto al jardín botánico - Floridablanca, Colombia.
http://www.casadeculturpiedradelsolgov.co | juridica@casadeculturapiedradelsol.gov.co

En el caso de utilizar foto de perfil la misma debe ser únicamente foto tipo carnet en donde se evidencie al funcionario.

La Dirección a través de la Oficina de Sistemas garantizará que todos los usuarios de correo electrónico institucional tengan configurada la firma con el estándar establecido.

3.7. Control de Acceso a los Datos.

Medios para impedir accesos no autorizados y registro de los accesos efectuados. Debe establecerse medidas de control de acceso a las dependencias Casa de Cultura Piedra del Sol y a los diferentes niveles de la plataforma tecnológica, tales como la red, sistema operativo y aplicaciones; así como a la información física que tenga un componente de seguridad.

Estas medidas estarán soportadas en el desarrollo de la cultura de seguridad de las personas que laboran en el organismo y buscarán limitar y monitorear el acceso a los activos de información requeridos para el trabajo, de acuerdo con su clasificación y manejando controles, en dispositivos y servicios que permitan identificar los niveles de acceso que los usuarios deben tener.

La Dirección General a través de la Oficina de Sistemas deberá elaborar, mantener y publicar los documentos de *servicios de red que ofrece la casa de cultura* a la planta de personal,

La Dirección General a través de la Oficina de Sistemas debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El control de las contraseñas de red y uso de equipos es responsabilidad de la Dirección General a través de la Oficina de Sistemas. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por La Dirección General a través de la Oficina de Sistemas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos a la Dirección General a través de la Oficina de Sistemas las cuales deben ser conservadas por la Dirección General y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Como requisito para la terminación de relación contractual o laboral del personal de la casa de cultura, la Oficina de Sistemas 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.

Los funcionarios serán responsables de realizar un adecuado uso de las herramientas de seguridad que se ponen a su disposición.

3.8. Adquisición, Desarrollo y Mantenimiento de Software.

Controles para garantizar que la Política de Seguridad esté incorporada a los sistemas de información. Asegurar que se haga un adecuado análisis e implementación de los requerimientos de seguridad del software desde su diseño, ya sea interno o adquirido, que incluya garantías de validación de usuarios y datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta. Además, se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida por parte de un usuario del sistema. Igualmente, se deberán asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
La implantación de nuevas herramientas de Hardware y Software, de sistemas de información y de otros recursos informáticos, deben cumplir con las políticas definidas.

3.9. Gestión de Incidentes.

Procedimiento a seguir en caso de suceder ciertos incidentes. Existe una clasificación de los incidentes según el grado en que afecten el normal funcionamiento del negocio. Controles para gestionar las incidencias que afectan a la seguridad de la Información. Asegurar que se haga una adecuada evaluación del impacto en el organismo frente a los eventos de seguridad relevantes, en los cuales las políticas de seguridad hayan sido desatendidas o traspasadas y realizará planes de atención de incidentes y mejora de procesos, para aquellos eventos que resulten críticos para la supervivencia del mismo. Estos planes deben considerar medidas: técnicas, administrativas y de vínculo con entidades externas, deben probarse y revisarse periódicamente, así como estar articulados en todo el organismo con los diferentes tipos de recursos tecnológicos y no tecnológicos.

3.10. Continuidad del Negocio.

Controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra averías y siniestros mayores. Se debe evaluar el impacto de los diferentes procesos en el organismo y realizar planes de mitigación y continuidad para aquellos que resulten críticos. Los planes de mitigación y continuidad deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente, y deben permanecer articulados con los diferentes recursos tecnológicos y no tecnológicos existentes en todo el organismo.

3.11. 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 de la Casa de Cultura Piedra del Sol.

4. RESPONSABILIDADES

4.1. Comité de Seguridad de la Información.

• Garantizar la existencia de una dirección y apoyo gerencial que soporte la administración y el desarrollo de iniciativas sobre seguridad de la información, a través de compromisos y uso adecuado de los recursos en el organismo.

• Formular y mantener una política de seguridad de la información que aplique a toda la organización conforme con lo dispuesto por Casa de Cultura Piedra del Sol.

• En todo caso, dicho comité o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a la Dirección de la Casa de cultura Piedra del Sol para su aprobación mediante resolución o acto jurídico correspondiente.

4.2. Grupo de Apoyo a la Seguridad.

• Desarrollar, mantener y administrar operativa y técnicamente la seguridad de la información conforme con las políticas de seguridad adoptadas por Casa de Cultura Piedra del Sol

• Materializar las medidas de largo, mediano y corto plazo que permitan el desarrollo efectivo, estratégico y armónico de las políticas planteadas.

4.3. Oficina De Recursos Humanos

El Director de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula por nombramiento o contractualmente con la Casa de Cultura piedra del sol, 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 Sistema de Gestión de la Seguridad de la Información.

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 según lineamientos dictados por el Comité de Seguridad de la Información.

4.4. Oficina Asesora Jurídica

El jefe de la Oficina Asesora Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información

4.5. Funcionarios Públicos, Contratistas y Particulares con acceso a información de la Casa de Cultura Piedra del Sol.

• Cumplir con todas las políticas de seguridad adoptadas por la **Casa de Cultura Piedra del Sol.**

• Actualizarse en los temas propios de seguridad de activos de la información aplicados en la Casa de Cultura Piedra del Sol

• Acuerdos de confidencialidad [ISO/IEC 27001:2005 A.6.1.5]

• Todos los funcionarios de la Casa de Cultura Piedra del Sol, contratistas y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la entidad , los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

• Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la Casa de Cultura Piedra del Sol, a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso contractual, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hará parte integral de cada uno de los contratos

4.6. Oficina de Control Interno

• La Oficina de Control Interno será la responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

5. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.

La Casa de Cultura Piedra del Sol, garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada ***Comité de Seguridad de la Información*** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Líder de Seguridad Informática de la Casa de Cultura.
- Un (a) Asesor de Dirección, Líder Gobierno Digital de la entidad.
- Secretario (a) General, o su delegado que deberá ser funcionario del área de sistemas
- Jefe (a) Oficina Jurídica o su delegado
- Secretario(a)
- Un Representante del Área de Archivo

6. REFERENCIAS

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

ISO/IEC 133351: 2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones.

ISO/IEC TR 133353: 1998. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI.

ISO/IEC 133354: 2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.

ISO 14001:2004. Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso

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

ISO/IEC 19011:2002. Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental

ISO/IEC Guía 62:1996 Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.

ISO/IEC Guía 73:2002. Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares.

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

ISO 9001:2000. Sistemas de gestión de calidad – Requerimientos.
ANEXO 5. Formato política SGSI modelo de seguridad de la información Gobierno Digital 2.0

DIRECTOR CASA DE CULTURA PIEDRA DEL SOL FLORIDABLANCA SANTANDER

Elaboro: Sindy Sabina Gamboa Pedraza.
Contratista CCPS
Aprobó: Jorge Enrique Gualdron Martínez.
Director CCPS

POLITICA DE SEGURIDAD DE LA INFORMACION PARA LA CASA DE CULTURA PIEDRADELSOL