**Políticas de Seguridad de la Información**

**Asociación Aeropuerto del Café**

**2023**

1. **INTRODUCCION**

Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos) y correo electrónico) y personas que interactúan haciendo uso de los servicios asociados a ellos. Asimismo, contribuir al cumplimiento de la misión y objetivos estratégicos de la Entidad, teniendo como base la seguridad de la información en cuanto a confiabilidad, disponibilidad e integridad.

1. **PROPOSITO**

Este documento de las Políticas de Seguridad y Privacidad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la ASOCIACIÓN AEROPUERTO DEL CAFÉ, para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información. Estarán obligados a dar cumplimiento a las presentes políticas emitidas y aprobadas por la ASOCIACIÓN AEROPUERTO DEL CAFÉ aquí descritas.

1. **GLOSARIO**

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones:

* **Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, oficinas, personas) que tienen un valor para la entidad.
* **Activo de Información:** de acuerdo con la norma ISO 27001, un activo de información es “cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido”. No obstante, este concepto es bastante amplio, y debe ser limitado por una serie de consideraciones: el impacto que para la Entidad supone la pérdida de confidencialidad, integridad o disponibilidad de cada activo, el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores. Los activos de información se traducen en dispositivos tecnológicos, archivos, bases de datos, documentación física, personas, sistemas de información, entre otros.
* **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
* **Áreas Seguras:** Son aquellas en donde se encuentren sistemas de procesamiento y almacenamiento informático o de datos. En la ASOCIACIÓN AEROPUERTO DEL CAFÉ se identifican las siguientes áreas seguras:

Cuarto de comunicaciones.

Cuarto de servidores.

Gabinetes con carpetas de información de contratos.

Lugares que contengan información Reservada

* **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
* **Cuarto de comunicaciones:** son lugares donde se deberán instalar los dispositivos de comunicación y el cableado. Al igual que los Centros de Cómputo, los Centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
* **Cuarto de servidores:** son cuarto zonas específicas para el almacenamiento de servidores para un fin específico. Los Centros de Cómputo deben cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
* **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
* **Confidencialidad:** es la garantía de que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella.
* **CSIRT:** Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
* **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
* **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
* **Incidente de Seguridad:** es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación o inminente amenaza de violación de una política o norma o de seguridad.
* **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
* **Integridad:** es la protección de la exactitud y estado completo de los activos.
* **Licencia de software:** es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
* **Mesa de ayuda:** Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de servicio que la Dirección de Información y Tecnología se informa de las necesidades que tienen los funcionarios en cuanto a los recursos informáticos.
* **Plan de Continuidad:** es el resultado de la aplicación de una metodología para crear y validar los planes orientados a la recuperación y restauración de las funciones criticas de una organización o Unidad organizacional, parcial o totalmente interrumpidas, dentro de un tiempo predeterminado después de una interrupción, emergencia o desastre.
* **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
* **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Entidad.
* **Registros de Auditoría**: son archivos donde son registrados los eventos que se han identificado en los sistemas de información y recursos tecnológicos de la Entidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
* **Responsable de Seguridad de la información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política, coordinar el Comité́ de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así́ lo requieran.
* **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
* **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por GOBERNACIÓN DE CALDAS o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de esta.
* **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, redes de datos o sistemas de información.
* **Vulnerabilidades:** son las debilidades, agujeros de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Entidad (amenazas), las cuales se constituyen en fuentes de riesgo.
* **VPN:** red virtual privada por sus siglas

1. **POLÍTICA GENERAL DE SEGURIDAD DE INFORMACIÓN**

Las Políticas de Seguridad y Privacidad de la Información, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la ASOCIACIÓN AEROPUERTO DEL CAFÉ sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

La ASOCIACIÓN AEROPUERTO DEL CAFÉ, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la ASOCIACIÓN AEROPUERTO DEL CAFÉ, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

* 1. **POLITICAS GENERALES**
* Los recursos informáticos solo pueden ser utilizados por los usuarios y contratistas u otros usuarios que cuentan con la debida autorización de la Gerente y Coordinador Administrativo y Financiero.
* Las políticas de tecnologías de información serán aprobadas por parte de la Gerencia y la socialización estará a cargo del Coordinador Administrativo y Financiero en acompañamiento con el contratista para el apoyo en el área de sistemas, estas políticas serán incluidas en los procesos de inducción.
* Los nuevos proyectos que tengan que ver con el uso de recursos tecnológicos serán validados y liderados por el área administrativa y financiera en acompañamiento con el contratista para el apoyo en sistemas.
* La adquisición de hardware y/o software serán validados por el contratista en apoyo de sistemas.
* Verificar que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas.
* El área de sistemas debe velar por la debida privacidad y confidencialidad en la plataforma e infraestructura tecnológica de la Entidad y solo se permitirá el acceso a información propia de los usuarios de la Asociación cuando sea solicitado de manera formal por una autoridad competente y con la respectiva justificación.
* El contratista en sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de las políticas de seguridad.

**RESPONSABILIDADES DE LOS USUARIOS**

* El equipo asignado es de uso personal por lo tanto cada usuario es responsable de este y del buen uso que le dé.
* Los usuarios tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
* No realizar cambios en las configuraciones de hardware o software instalado en los equipos de cómputo ya que este solo lo realiza el área de sistemas.
* A no divulgar la clave de acceso ya que esta es de uso personal e intransferible, como consecuencia se entiende para todos los efectos que solo la conoce el responsable del equipo y el contratista de Sistemas.
* El usuario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al área de sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
* Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las directivas, el usuario informático deberá notificar al área de sistemas.
* Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información debe ser reportado al área de sistemas.
* Los usuarios tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
* Los usuarios no deben interferir en los procesos computacionales de la Asociación ni en el buen funcionamiento de los servicios y recursos de la misma mediante acciones deliberadas que disminuyan el desempeño o la seguridad de los equipos instalados. Se considerará justa causa de terminación del contrato el manejo indebido de los sistemas de tecnología.
* Está prohibido mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, o retirar sellos de los mismos. Lo anterior es responsabilidad exclusiva del área de sistemas, por lo tanto, en caso de requerir este servicio deberá solicitarlo.
* Es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Los usuarios pueden pedir apoyo al área de sistemas para el uso de antivirus.

**LICENCIAMIENTO DE SOFTWARE.**

* Todo software adquirido para el uso de la Asociación debe estar debidamente licenciado y es responsabilidad directa del área de sistemas cumplir la norma.
* La adquisición de cualquier software debe tener el aval y aprobación de la Coordinación Administrativa y Financiera y la Gerencia con el apoyo de la contratista de sistemas.
* El área de sistemas debe realizar al menos dos veces al año inspecciones a los equipos de la Asociación para asegurarse que el software instalado en los computadores se encuentre debidamente licenciado.
* Todos los productos de software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

**DERECHOS DE AUTOR**

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Asociación bajo ninguna circunstancia sin la autorización escrita del área de sistemas. No está permitido instalar ningún programa en su computadora sin la autorización escrita del área de sistemas.

* Está prohibido realizar intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
* Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
* Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

**SOPORTE (MESA DE AYUDA DE LOS PROVEEDORES A LOS RECURSOS INFORMÁTICOS DE LA ENTIDAD)**

* Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora, y con los programas remotos autorizados por el área de sistemas.

**EQUIPO DE COMPUTO**

* Para el correcto funcionamiento del equipo de cómputo deberá realizarse como mínimo mantenimientos preventivos cada año, de acuerdo al plan de mantenimiento preventivo elaborado por el área de sistemas.
* El área de sistemas será el encargado de asignar el equipo de cómputo.
* Deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.
* El área de sistemas instalará todas las aplicaciones de los equipos y programas informáticos utilizados por la Asociación.
* El área de sistemas llevará inventario de hardware y software (programas) instalados en la Asociación.

**SEGURIDAD**

Seguridad del recurso humano

* Todo el personal nuevo de la Asociación, deberá ser notificado al área de sistemas por la coordinación Administrativa y Financiera de tal forma que se asigne los recursos correspondientes (Equipo de cómputo, creación de usuario para la red, creación de usuario para el correo electrónico y creación de usuario en la plataforma de Microsoft 365) o en caso de retiro, anular y cancelar los derechos otorgados como usuario informático.
* Todos los usuarios empleados, contratistas deberán devolver todos los activos de la Asociación que tengan a su cargo a la terminación de su empleo o contrato.
* El acceso al centro de datos es restringido y solo personal autorizado por el área de sistemas puede tener acceso a él.
* El acceso a los servidores de la Asociación ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por el área de sistemas
* Asear semanalmente el cuarto de comunicaciones y el cuarto de servidores (archivos y financiero), que permita mantenerse libre de polvo.
* Se debe revisar constantemente las instalaciones eléctricas y red de datos para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
* Contar con UPS de respaldo para la continuidad del servicio.
* Contar por lo menos con un extintor de incendio adecuado y cercano al centro de datos.
* Los equipos electrónicos de gestión e infraestructura de la red de La Asociación serán instalados, configurados y mantenidos exclusivamente por el área de sistemas.
* No es permitido a ningún funcionario, excepto el área de sistemas, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
* El área de sistemas es la responsable de proporcionar a los usuarios el acceso a los recursos de conectividad.
* Los usuarios deben guardar la información en las carpetas asignadas para garantizar que dicha información sea respaldada.
* Diariamente se realizan respaldos automáticos a la información almacenada en las carpetas que tiene asignada cada usuario en los equipos de computo, al servidor de archivos y financiero mediante la herramienta SyncBackFree la cual envia la información al dispositivo QNAS a través de la red
* Los equipos deberán ser bloqueados por cada usuario en el momento en que deje de utilizar el pc para evitar accesos no autorizados.
* las sesiones de Windows personales estarán protegidas con contraseña.
* Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.
* No es responsabilidad del área de sistemas la perdida de información personal que se encuentre en cada equipo
* Todo acceso a la información de la Asociación deberá tener las respectivas autorizaciones y accesos, que garanticen su respectiva seguridad, integridad y confidencialidad de la información almacenada.
* Los funcionarios deben realizar revisiones periódicas de su información almacenada con el fin de no mantener información innecesaria.
* Se debe realizar copia de seguridad (Backup) del software financiero, y carpetas compartidas en el servidor publico, con el propósito de salvaguardar la información. Estas se deben realizar diariamente por el área de sistemas y se deberán almacenar en un sitio externo al edificio (se almacena en los servidores de la Gobernación de Caldas).

**USO DE INTERNET**

En caso de que se identifique que algún acceso que se solicite amenace la seguridad de la información de la Asociación no se concederán los permisos, tales como accesos remotos, VPN externas, carpetas públicas.

Prohibiciones de internet.

* Páginas con contenido pornográfico.
* Descargue de ninguna aplicación sin autorización del área de sistemas.

**CORREO ELECTRÓNICO**

Teniendo en cuenta que el correo electrónico es una herramienta que provee la empresa para el cumplimiento de las funciones, toda la información manejada y almacenada es propiedad de la Asociación Aeropuerto del Café incluyendo las copias de seguridad del mismo.

* Semanalmente cada usuario es responsable de eliminar los correos de la papelera, spam y correos que ya no son necesarios tenerlos en el correo para evitar que se llene el espacio de almacenamiento.
* Se debe descargar los archivos adjuntos con tamaño mayor a 2 Megas y almacenarlos en la capeta local de cada usuario.

**RENOVACIÓN DE EQUIPOS**

Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

* Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por (5 años) sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de sistemas a fin de que se seleccione el equipo adecuado. Sin el visto bueno del área administrativa y financiera no podrá realizarse el proceso de contratación u orden de compra.

**ELABORADO POR:**

**Contratista Ingeniera de Sistemas: ELIANA GARCÍA VÉLEZ**