POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

AEROPUERTO INTERNACIONAL SANTA ANA S.A.

OBJETIVOS

OBJETIVO GENERAL

La política de Seguridad Informática tiene como objetivo principal, establecer reglas claras sobre el buen uso de los sistemas informáticos y de comunicaciones del Aeropuerto Internacional Santa Ana por parte de usuarios, administradores o terceros. De igual manera, proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

OBJETIVO ESPECIFICO

- ✓ Busca establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red y acceso físico.

- ✓ Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

ALCANCE

Esta Política abarca todo el ámbito del Aeropuerto Internacional Santa Ana, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados del Aeropuerto Internacional Santa Ana a través de contratos o acuerdos con terceros. Ningún empleado, funcionario, contratista, departamento, grupo, oficina, comité, organización o unidad operativa está exenta de estas políticas.

De igual manera comprende a los datos e información del Aeropuerto Internacional Santa Ana, sin importar la presentación o formato de almacenamiento ni su localización, propósito, consideraciones de custodia o uso original.

DEFINICIONES

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

✓ **Confidencialidad:** Garantizar que todos los recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales. Asegurar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

✓ **Integridad:** Establecer mecanismos y métodos de procesamiento para garantizar que toda la información que se maneje se encuentre libre de errores y/o corrupción por personas o procesos no autorizados. Salvaguardar que la información se mantenga con exactitud, tal como fue generada, sin ser manipulada ni alterada.

✓ **Disponibilidad**: Garantizar que la información se encuentre sólo a disposición de las personas, procesos o aplicaciones que deben tener acceso a ella y en el momento que así lo requieran.

✓ **Información:** Conjunto de datos procesados y organizados.

✓ **Amenaza:** Circunstancia que tiene el potencial de causar daño o una perdida. Las amenazas pueden materializarse dado el lugar a un ataque en un equipo.

✓ **Vulnerabilidad:** debilidad d un sistema de información que puede ser utilizado para causar daños específicos.

✓ **Riesgo:** Posibilidad que una amenaza se materialice, dando a lugar un ataque a un componente tecnológico.

APLICABILIDAD

Esta política aplica para todos los funcionarios, contratistas, personal temporal, practicantes y demás personas que ingresen a los sistemas de información o instalaciones del Aeropuerto Internacional Santa Ana

MARCO NORMATIVO

- Ley 527 de 1999, Por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
- Ley 599 de 2000, Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- Ley 594 de 2000, Ley general de Archivos.
- Ley 962 de 2005, Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Ley 1150 de 2007, Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009, Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- Ley 1437 de 2011, Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013, 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.
- Ley 1755 de 2015, Por medio del cual se regula el derecho fundamental de petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Decreto 2693 de 2012, Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de

Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones

- Decreto 2578 de 2012, Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- Decreto 2609 de 2012, Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 1081 de 2015, Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- Decreto 1166 de 2016, Por el cual se adiciona el capítulo 12 al Título 3 de la Parte 2 del Libro 2 del Decreto 1069 de 2015, Decreto Único Reglamentario del Sector Justicia y del Derecho, relacionado con la presentación, tratamiento y radicación de las peticiones presentadas verbalmente.
- Decreto 1499 de 2017, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Y se realiza la Actualización del Modelo Integrado de Planeación y Gestión. CAPÍTULO 3: Modelo Integrado de Planeación y Gestión, Artículo 2.2.22.3.5· Manual Operativo del Modelo.
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 3564 de 2015, Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Resolución 60362 de 2017, Por la cual se adopta la Política General de Seguridad de la Información para el Aeropuerto Internacional Santa Ana.
- ISO/IEC TR 18044:2004, Ofrece asesoramiento y orientación sobre la seguridad de la información de gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.
- BS 7799-3:2006, Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe

cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

- NTCGP1000:2009, Esta Norma establece los requisitos para la implementación de un sistema de gestión de la calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicio.
- NTC 27001:2013, La norma ISO 27001, es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El Estándar 27001:2013, para los Sistemas de Gestión de Seguridad de la Información, permite a las organizaciones la evaluación del riesgo de Seguridad de la información y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
- ISO 27002:2013, Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.
- CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada desde la Presidencia de la República y el MinTIC, para orientar y dar los lineamientos respectivos a las entidades.

POLITICAS.

SEGURIDAD DE INFORMACIÓN SENSITIVA

- Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que maneje, especialmente si dicha información ha sido clasificada como sensible.

- Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral en el Aeropuerto internacional Santa Ana, no podrán facilitarla más que a aquellos otros empleados que necesiten conocerla para la misma finalidad y se abstendrá de usarla en beneficio propio.

- La información clasificada como no publicable debe ser tratada de manera que se garantice su secreto, reserva o confidencialidad según sea el caso. Los usuarios solamente podrán revelar esta información a los jefes de sus respectivas áreas, salvo cuando la información la sea solicitada por la autoridad judicial en virtud de

providencia dictada en juicio. Los usuarios serán responsables en los términos de la ley por la violación del secreto que se establece y estarán obligados, en caso de revelación de secreto, a reparar los daños y perjuicios que se causen.

- La información relativa a los empleados, funcionarios, contratistas y personas en general, incluida, en su caso, la relativa a remuneraciones, evaluaciones y revisiones médicas debe ser tratada con especial cuidado como Información Confidencial sensible del Recurso Humano.

- La información de políticas, normas, procedimientos y lo relacionado con la estrategia de producto, comercialización, penetración de mercado, tarifas, y demás aspectos que caracterizan los productos, servicios y/o procesos deben ser consideradas como privativas del Aeropuerto internacional Santa Ana y su uso sin autorización viola derechos de autor.

- Es responsabilidad de los usuarios garantizar que toda documentación en formato impreso, electrónico, etc., que contenga información sensitiva de Vigilados y Usuarios una vez utilizada, o que no pueda ser entregada al Vigilado o a los Usuarios, es archivada de manera segura o pasa a destrucción.

- Es responsabilidad de los usuarios el resguardo de toda aquella información clasificada como no publicable en documentación física o electrónica que por carácter regulatorio sea considerada secreta, reservada o confidencial según sea el caso.

- Se prohíbe todo envío de información que por carácter regulatorio sea considerada secreta, reservada o confidencial, aun cuando sea entre usuarios de las mismas áreas; en caso de ser requerido su envío, debe ser autorizado por el Aeropuerto Internacional Santa Ana y citado como función en el contrato o resolución de nombramiento, adicionalmente debe cifrarse a través de medios electrónicos de transferencia como lo son: servicios de correo electrónico, Mensajería instantánea, chat.

- Es responsabilidad de los encargados de la gestión de archivos físicos, velar por la integridad de la información almacenada físicamente. Todas las dependencias almacenan los archivos físicos por un tiempo determinado después de eso pasan al área de Gestión Documental, (archivo general), todo de acuerdo a las TRD contextualizadas por el Archivo General de la Nación, bajo la ley 594 de 2000.

- Cuando se traslade documentación física considerada secreta, reservada o confidencial por parte de cualquier empleado del Aeropuerto Internacional Santa Ana y/o tercero, ya sea que ingrese o salga de las oficinas o transite entre las áreas, debe portar los expedientes y demás documentos dentro de un fólder o bolsa cerrada que no permita ver el contenido de los mismos (impedir la visión de la información).

- Es responsabilidad de los usuarios que aquella papelería que contiene datos considerados secretos, reservados o confidenciales, sea cortada adecuadamente para su desecho, no se debe permitir su reutilización.

- Es responsabilidad de los jefes de área, que todo dispositivo del Aeropuerto Internacional Santa Ana que almacene información considerada secreta, reservada o confidencial, en cualquier medio (papel, cintas, PC, servidores, etc.) debe ser registrado en la matriz de información clasificada y reservada, definida por la entidad.

- Es responsabilidad del Comité de Gestión y Desempeño realizar al menos semestralmente revisiones sobre el cumplimiento de la matriz de información clasificada y reservada y/o la necesidad de actualizar la misma.

- Es responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones, asegurarse que los equipos de almacenamiento o respaldo de información que deban ser desechados, se destruyan físicamente o sean escritos de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no queda información permanente.

- Es responsabilidad del Usuario almacenar la información crítica en las carpetas compartidas dispuestas a través de la red, para tal fin, estas se encuentran organizadas por cada una de las áreas y administradas por el Grupo de Tecnologías de la Información y las Comunicaciones.

- Debe usarse cadena de custodia para información clasificada como sensible, basada en las normas de la Policía Judicial.

USO DE LAS ESTACIONES DE TRABAJO

- El Usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario. El área responsable deberá mantener los registros de inventario debidamente actualizados.

- Se prohíbe utilizar la Información, Hardware, Software y Acceso a Internet (redes de comunicación o TIC), para realizar actividades diferentes a las estrictamente laborales.

- Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera del Aeropuerto Internacional Santa Ana sin la debida autorización escrita y extendida por el responsable que corresponda y debe estar motivado por los intereses y objetivos Aeropuerto Internacional Santa Ana. La dependencia a la que le corresponde esta labor es el Gerente.
- Se prohíbe instalar y utilizar en el Hardware, Software no autorizado o software ilegal. En los equipos del Aeropuerto Internacional Santa Ana sólo podrá instalarse y utilizarse software legal y oficial. No se debe modificar la configuración de Hardware y Software establecida por el Grupo de Tecnologías de la Información y las Comunicaciones. No está permitido hacer copias del software para fines personales.
- Ninguna información del Aeropuerto Internacional Santa Ana podrá utilizar tecnologías de computación o almacenamiento en la nube si no está dentro del portafolio de servicios provistos por el Grupo de Tecnologías de la Información y las Comunicaciones y regulados dentro de la estructura de almacenamiento de la Entidad.
- Se prohíbe instalar en el Hardware del Aeropuerto Internacional Santa Ana, software propiedad del usuario, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por las directivas del Aeropuerto Internacional Santa Ana, en este caso el Coordinador de área del usuario solicitante, debe registrar la incidencia sobre la plataforma de soporte mediante LA MESA DE TRABAJO, que documente la acción, con el objeto de que el personal de soporte proceda a proporcionar la solución adecuada.
- La entidad, es responsable de utilizar un protector de pantalla con contraseña para evitar que otras personas ingresen a sus archivos. Así mismo, siempre que sea posible el Hardware deberá estar instalado de tal forma que no permita que visitantes o personas extrañas a El Aeropuerto Internacional Santa Ana puedan tener acceso a ningún tipo de información, ya sea en pantalla, impresora o cualquier otro dispositivo.
- El Usuario es responsable de bloquear su estación de trabajo durante cualquier ausencia temporal de su puesto de trabajo.
- El Usuario es responsable de mantener el escritorio físico limpio y organizado: Si este se encuentra desordenado, es muy probable que no se pueda identificar la pérdida de algún elemento. Los documentos del Aeropuerto Internacional Santa Ana, deberán estar disponibles únicamente a personas autorizadas y bajo la responsabilidad del custodio que salvaguarda la información.

- Es responsabilidad del Usuario recoger, almacenar y asegurar bajo llave el material físico sensible al finalizar la jornada de trabajo y/o cuando se ausente de su puesto de trabajo: Los usuarios deberán tomarse el tiempo necesario antes de abandonar la oficina correspondiente y/o ausentarse de su puesto de trabajo, no deben reposar carpetas, ni oficios en los escritorios, estos deben ser salvaguardados bajo llave.
- Es responsabilidad del área de Recursos Humanos y el área Administrativa los Contratos, reportar al Grupo de Tecnologías de la Información y las Comunicaciones tan pronto un empleado termine su relación con el Aeropuerto Internacional Santa Ana o cuando un empleado solicite vacaciones o suspensión temporal del contrato, para que se realicen las labores correspondientes a nivel de acceso a sistemas de información y aplicativos de la entidad.:
- El Usuario es responsable de mantener organizado el disco duro del equipo de cómputo que le fue asignado por el Aeropuerto Internacional Santa Ana, y conservar en el mismo únicamente los archivos que necesita para llevar a cabo sus labores. Los archivos de uso personal están restringidos y estarán bajo la responsabilidad del Usuario.
-Se prohíbe el uso del Hardware y Software del Aeropuerto Internacional Santa Ana a terceros o personas externas al mismo, salvo autorización previa emitida por el Coordinador de área a la que pertenezca.

- En este caso, al momento de crear la incidencia en el LA MESA DE TRABAJO, se debe aclarar que se permite el uso del equipo propiedad del usuario para que el personal de soporte, posteriormente realice las respectivas configuraciones y habilite los accesos de red, pertinentes.

- Es responsabilidad de los usuarios identificar y reportar al gerente del Aeropuerto Internacional Santa Ana, el hardware y software no autorizado, así como la pérdida o robo de los mismos.
- Es responsabilidad del usuario no dejar desatendido en ningún momento el Hardware, sobre todo si se está imprimiendo o se va a imprimir Información Confidencial.
- Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:

♣ No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.

♣ No colocar objetos pesados encima del Hardware. Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc., que puedan afectar los componentes de los equipos.

♣ No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente.

♣ No abrir el Hardware. De ser necesaria dicha labor, será llevada a cabo por un experto.

♣ Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
♣ Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos. 6.2.17 Política complementaria de acceso remoto (Remote Access) Proteger la información a la que se tiene acceso, que es procesada y/o almacenada en los lugares en los que se realiza Teletrabajo y/o Acceso Remoto, para salvaguardar la confidencialidad y privacidad de la misma.

USUARIOS Y CONTRASEÑAS

- Es responsabilidad del Gerente la administración de usuarios, asignar un nombre único de usuario, y es responsabilidad del usuario tener una contraseña robusta reservada en cada sistema informático, los cuales deberán ser confidenciales e intransferibles para garantizar su óptima identificación. (Revisar numeral 6.3.13).

- La asignación de credenciales de identificación de usuario genérico o universal deberá ser documentada y administrada por el Grupo de Tecnologías de la Información y las Comunicaciones. Esta documentación deberá tener como mínimo los nombres, cargos y la utilización que se le dará a la cuenta por parte de los usuarios.

- Se prohíbe asignar credenciales de identificación de usuario a personas que no sean empleados del Aeropuerto Internacional Santa Ana, a menos que estén debidamente autorizados, se determinen los medios de control requeridos, se evalúe el riesgo y sean por tiempo limitado.

- Ningún usuario o programa debe utilizar las contraseñas de administrador, salvo personal autorizado.

-Las credenciales de Identificación de Usuario deben ser modificadas por el usuario mediante el inicio de sesión de cada uno de los mismos, este cambio se realiza cada 60 días, en el caso de que no sean usadas por un período de un (1) mes, deben ser inactivados.

- Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona.

- Es responsabilidad del Usuario no usar contraseñas que sean idénticas o sustancialmente similares a contraseñas previamente empleadas.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para el primer inicio de sesión. Es responsabilidad del Usuario cambiar en esta primera sesión su contraseña inicial por otra contraseña de acuerdo a los parámetros de creación de credenciales de acceso, dispuestos en el numeral 5.3.13.

- Las contraseñas para el uso de aplicaciones externas deben ser autorizadas por el Gerente.

- Se limita a tres (3) el número consecutivo de intentos infructuosos para introducir la contraseña de Usuario; después del tercer y último intento la cuenta involucrada queda bloqueada. Para realizar el respectivo desbloqueo de la cuenta, debe realizar la respectiva incidencia por medio del LA MESA DE TRABAJO, para que procedan a desbloquear el equipo.

- Es responsabilidad del Usuario evitar que su contraseña esté visible en pantalla, cuaderno o libreta en cualquiera de los procesos en que la utilice (conexión, utilización, etc.).

- Se prohíbe tener múltiples sesiones de usuario en diferente Hardware.

- Es responsabilidad del Usuario crear siempre contraseñas robustas, para ello, las credenciales de acceso se deben generar bajo las siguientes condiciones:

- El usuario debe cambiar la contraseña en la primera vez de uso.
- La contraseña debe tener como mínimo 7 caracteres.
- Se genera una solicitud de renovación de credencial de acceso cada 45 días.
- No deben contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- La contraseña debe tener caracteres Mayúsculas y Minúsculas, dígitos del 0 al 9 y caracteres no alfanuméricos(!, $, #, %).

- Es responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones, realizar una revisión periódica de al menos dos veces al año, de los accesos asignados a los usuarios.

- El control de acceso a de los usuarios a la red, se controla por medio del tiempo de servicio pactado en cada uno de los contratos laborales.

- Se requiere de la creación de una incidencia por medio del LA MESA DE TRABAJO, solicitando autorización para todo acceso, debe detallar los privilegios solicitados y debe ser autorizado por el Gerente de acuerdo con los procedimientos vigentes.

- En caso de que un correo institucional sea usado por varios empleados y algún empleado ya no tenga un vínculo laboral con la entidad, el custodio deberá informar al Grupo de Tecnologías de la Información y las Comunicaciones para realizar el respectivo cambio de contraseña de correo.

- Se debe portar el carnet de la entidad en un lugar visible.

6.4 POLÍTICA DE EVALUACIÓN DE RIESGOS

- Es responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones, que se ejecute al menos una vez al año un Test de Penetración tanto interno como externo, dichos análisis deben de ser ejecutados por personal conocedor en temas de Ethical Hacking, utilizar herramientas adecuadas y tener experiencia importante en el tema. Una vez se tengan los resultados se deben gestionar las soluciones pertinentes para las vulnerabilidades encontradas.

- Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables. De acuerdo a la metodología de riesgos implementada en el Aeropuerto Internacional Santa Ana. Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar y evaluar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir y/o retener los riesgos.

El tratamiento de los riesgos de Seguridad de la información, se evaluará de acuerdo a la metodología de Tratamiento de Riesgos definida por la entidad.

POLÍTICA DE CONTROL DE CÓDIGO MALICIOSO

- Es responsabilidad del Usuario permitir la ejecución del Antivirus autorizado por el Aeropuerto Internacional Santa Ana, el cual tendrá disponible automáticamente cada vez que inicie sesión en el equipo asignado en el dominio de la red.

- Está terminantemente prohibido al Usuario ejecutar los archivos anexos a su correo electrónico si no provienen de una fuente reconocida y segura, una vez identificados deben ser reportados a la Mesa de Servicios del Grupo de Tecnologías de la Información y las comunicaciones.

- Es responsabilidad del Usuario dar aviso inmediato a la Mesa de Ayuda por medio del registro de una incidencia sobre el LA MESA DE SERVICIOS9 al detectar la presencia de un virus electrónico que no es eliminado por el Antivirus.

- Por motivo de seguridad, los mensajes que contengan virus serán inmediatamente eliminados sin posibilidad de recuperación.

- Es responsabilidad del usuario revisar con el antivirus sus unidades de almacenamiento en medios extraíbles antes de usarlas. Es responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones, que todos los sistemas aplicables sean configurados con el antivirus corporativo con parámetros configurados para recibir actualizaciones automáticas y realizar escaneos periódicos.

POLÍTICA DE USO DE CORREO ELECTRÓNICO

- Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; este tipo de mensajes sólo puede ser enviado por usuarios debidamente autorizados. Los usuarios autorizados son: el funcionario autorizado por la Secretaría General.

- Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores del mismo,

tales como comentarios sobre sexo, raza, religión o preferencias sexuales; igualmente redactar un correo en mayúsculas, aumentar el tamaño del texto, etc, son considerados como hablar en un tono de voz muy fuerte en los correos; así mismo, es responsabilidad del Usuario reportar a su Jefe de área la recepción de este tipo de mensajes, quien a su vez deberá reportarla al Grupo de Tecnologías de la Información y las Comunicaciones, en su caso.

- Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por otro funcionario o terceros (clientes o proveedores).

- Es responsabilidad del Usuario evitar que la información confidencial sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa emitida por la Alta dirección, en cuyo caso los archivos deben viajar en forma Segura.

- Es responsabilidad del Usuario evitar el uso de una cuenta de correo electrónico que pertenezca a otro usuario, si hay necesidad de hacerlo en caso de ausencias o vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes.

- Se considera uso inapropiado de la cuenta de correo electrónico, lo siguiente:

- Enviar mensajes desde la cuenta de correo electrónico de un usuario con firma de otro.
- Intentar acceder sin autorización a otra cuenta de correo electrónico.
- Transmitir mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización expresa del propietario de la información.
- Participar en cadenas de mensajes que congestionen la red.

- Es responsabilidad de los usuarios de correo electrónico gestionar o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

- Todos los mensajes enviados por medio de correo electrónico pertenecen a el Aeropuerto Internacional Santa Ana y éste se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

- Todos los correos institucionales tendrán un custodio quién es el encargado de administrar y asegurar el buen uso del mismo. 5.6.10 Todos los correos electrónicos entrantes y salientes serán analizados para evitar que tengan virus. Si se evidencia

virus, el correo será enviado a cuarentena y se generará una alerta al Usuario indicando el tipo de amenaza.

POLÍTICA DE CONTROL DE CAMBIOS

- Es responsabilidad de todos los empleados del Aeropuerto Internacional Santa Ana, realizar el respectivo proceso de control de cambios, cada vez que soliciten la implementación de un nuevo sistema, modificación a uno existente o la implementación de cualquier cambio tecnológico, estas modificaciones deben ser solicitadas a la mesa de ayuda por medio del registro de incidencias en LA MESA DE TRABAJO

POLÍTICA DE MEDIOS DE ALMACENAMIENTO EXTRAÍBLES

- Los medios electrónicos que contengan información confidencial o sensible están sujetos a las siguientes directrices de almacenamiento:

✓ La información confidencial y sensible nunca debe copiarse en medios removibles sin una autorización previa del Gerente

✓ Los medios electrónicos que contengan datos confidenciales o sensibles del cliente deben ser físicamente retenidos, almacenados o archivados únicamente dentro de entornos de oficina seguros.

✓ Todos los medios electrónicos que contengan información confidencial y sensible deben etiquetarse claramente como tal.

✓ Todos los medios deben enviarse o entregarse por medio de un mensajero confiable u otro método de entrega que pueda rastrearse de modo preciso y deben ser aprobados por el Gerente.

✓ Es responsabilidad de los usuarios Administradores o Custodios de centros de almacenamiento de información (impreso o electrónico), mantener un registro de Inventario de Medios. Todos los medios impresos y electrónicos almacenados que contengan información confidencial o sensible deben ser inventariados por lo menos anualmente.

- Es responsabilidad de los Jefes de cada área, que la documentación en papel u otros medios que contengan información confidencial y se haya cumplido su período de retención, sean desechadas mediante un proceso que garantice la destrucción apropiada de dichos elementos.

POLÍTICA DE SEGURIDAD FÍSICA

- Todos los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.
- Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles proporcionados por el Aeropuerto Internacional Santa Ana, para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- ✓ El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.
- ✓ El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
- ✓ En el caso de los dispositivos usados para los operativos de transporte, se dispone de un protocolo que dispone el correcto y su operatividad dentro de la red.

POLÍTICA DE SEGURIDAD APLICABLE A LOGS

- Es responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones, que los logs generados sean monitoreados regularmente para detección temprana de posibles fallas en los equipos y aplicaciones o vulnerabilidades de seguridad.

POLÍTICA DE SEGURIDAD APLICABLE VPN

- Todos los usuarios que tengan acceso por medio de VPN a la red interna de del Aeropuerto Internacional Santa Ana deben estar debidamente autorizados y documentados, tanto por el jefe del área, como por el oficial de seguridad.

- Es responsabilidad de los usuarios que utilizan los servicios de VPN asegurar que otras personas no autorizadas accedan a las redes internas del Aeropuerto Internacional Santa Ana.

POLÍTICA DE BACKUPS DE LA INFORMACIÓN

Asegurar que la información generada por las diferentes unidades administrativas, esté disponible en caso de cualquier contingencia, como daño en los discos duros, o eliminación accidental de la Información

El Aeropuerto Internacional Santa Ana, cuenta una infraestructura que da cumplimiento a los requerimientos de salvaguarda de la información, la cual cuenta con el espacio, software y hardware adecuado. El procedimiento de Backups cubre los aspectos para la creación de copias de seguridad que debe realizarse por parte de los funcionarios del Grupo de Tecnologías de la Información y las Comunicaciones, para una adecuada aplicación y de acuerdo a las necesidades del Aeropuerto Internacional Santa Ana.

POLÍTICA DE ACCESO A INTERNET

Para el acceso de los usuarios a internet, se dispone un Firewall de tipo Perimetral, el cual permite controlar los permisos de los equipos a internet. En condiciones iniciales, la red se encuentra en un acceso restringido, el cual solo permite el ingreso a ciertas páginas, las cuales solo permiten al acceso al correo, realizar consultas generales en buscadores y acceso a páginas de contenido gubernamental, entidades bancarias y entidades de salud, de acuerdo al objeto de la entidad.

POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Conservar la disponibilidad de los procesos críticos del Aeropuerto Internacional Santa Ana y la continuidad de su operación, con base en los tiempos de recuperación y el impacto que puedan generar los eventos. Lineamientos Del propietario de los activos de información Determinar los requisitos de seguridad de la información que deben mantenerse durante una crisis o desastre, y debe realizar el Análisis de Impacto al negocio (BIA) para determinar, principalmente, los procesos y actividades críticas, con base en esto, establecer los controles que soportan los requisitos de seguridad de la información con el apoyo del Oficial de seguridad de la información.

Del Oficial de Seguridad de la Información o el Coordinador del Grupo de Tecnologías de la Información y las Comunicaciones.

- ✓ Identificar los escenarios más probables para el diseño de las estrategias de continuidad, de acuerdo con los resultados de la Valoración de Riesgos y el Análisis de Impacto al Negocio.

- ✓ Presentar las estrategias de continuidad viables, para ser evaluadas y aprobadas por la Coordinación de Informática en términos de recursos, tiempo e impacto.
- ✓ Desarrollar el cronograma de pruebas periódicas para cada una de las estrategias, pertinentes al plan de continuidad del negocio.
- ✓ Asegurar que cada Líder de proceso realice las pruebas de continuidad de acuerdo al cronograma establecido. Avalar las aplicaciones propias y adquiridas.
- ✓ Avalar despliegues e instalaciones.
- ✓ Los planes de continuidad se deben revisar mínimo una vez al año o cuando se presenten cambios significativos que puedan afectar la continuidad de seguridad de la información, dejando registro de la aprobación y revisión de los mismos, socializándolos a través de la comunicación al interior del Aeropuerto Internacional Santa Ana.
- ✓ Asegurar que el personal con responsabilidades en los planes, esté capacitado y entrenado en cada una de las actividades expuestas en el plan de continuidad de del negocio junto con los líderes de los procesos. 5.15 Política de Gestión de Incidentes de seguridad Garantizar que los incidentes de seguridad de la información se reportan, se toman acciones correctivas para su solución y se documentan de manera oportuna. Lineamientos De los colaboradores, servidores públicos, contratistas
- ✓ Reportar los incidentes de Seguridad de Información de los cuales tengan conocimiento, a través del Gerente del Aeropuerto Internacional Santa Ana.
- ✓ Responsabilizarse de las acciones legales y disciplinarias correspondientes según el caso, con base a los resultados de las investigaciones relacionados con los incidentes de seguridad de la Información.
- ✓ Cualquier hecho o evento que afecte la confidencialidad, integridad o disponibilidad de la Información, así como la violación a las Políticas de Seguridad de Información se considera un Incidente de Seguridad de Información, incluyendo:
    - Fuga, Robo o Pérdida de Información: Situación en la que no se puede acceder a datos y/o información a la cual se tenía acceso.
    - Alteración o Eliminación no autorizada de Información.
    - Indisponibilidad de los Servicios: No disponibilidad de los servicios en los tiempos acordados.

- Divulgación no autorizada de Información
- Presencia de virus, cadenas o correos basura
- Acceso no autorizado: Acceder de manera indebida, sin autorización o contra derecho a un sistema y/o plataforma tecnológica.
- Instalación de software ilegal o no licenciado: Contravención a derechos de autor.
- Préstamo de usuario y contraseña
- Ingreso de medios de almacenamiento no autorizados
- Información o actividades que atenten contra la propiedad intelectual o derechos de autor
- Ingeniería Social: Práctica para obtener información confidencial a través de la manipulación de usuarios legítimos.

De los colaboradores, servidores públicos, contratistas que realizan tareas de administración de sistemas de información, infraestructura y redes

✓ Activar los registros de auditoría de las plataformas tecnológicas para apoyar el proceso de investigación de Incidentes de Seguridad.

✓ Revisar las vulnerabilidades técnicas de los sistemas de información y la infraestructura del Aeropuerto Internacional Santa Ana, para identificar el nivel de riesgo, tomar las acciones necesarias para tratarlos y responder oportunamente.

De Seguridad de la Información

✓ Ejecutar como mínimo trimestralmente escaneos de vulnerabilidad (internos /externos) y/o después de cada cambio significativo en la red. Identificar las vulnerabilidades de las aplicaciones e infraestructura mediante el uso de herramientas para su detección y el acceso a la información de los proveedores, generando planes de acción.

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Proteger los datos personales de los ciudadanos, el Aeropuerto Internacional Santa Ana debe adoptar los niveles de seguridad de protección de los datos personales legalmente requeridos, instalando las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados, a través del cumplimiento de los siguientes principios:

✓ Principio de la Legalidad, tratar los datos personales, de acuerdo a lo establecido en la normatividad vigente.

✓ Principio de finalidad, indicar la finalidad del tratamiento de datos personales, informándolo al titular.

✓ Principio de libertad, tratar los datos solo con el consentimiento previo, expreso e informado del titular de los datos.

✓ Principio de veracidad o calidad, la información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

✓ Principio de transparencia, garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.

✓ Principio de acceso y circulación restringida, el tratamiento solo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.

✓ Principio de seguridad, la información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

✓ Principio de confidencialidad, garantizar la reserva del Tratamiento de Datos Personales por todos los colaboradores que participen en esta actividad.

POLÍTICA DE TERCERIZACIÓN U OUTSOURCING

- Se deberá aceptar y firmar el Acuerdo de Confidencialidad establecido por el Aeropuerto Internacional Santa Ana, por las terceras partes que realicen un vínculo contractual, convenio o acuerdo con la entidad.
- En todos los contratos, convenios o acuerdos con terceras partes se debe incluir una causal de terminación, por el no cumplimiento de las políticas de seguridad de la información.
- La información relacionada o que surja del contrato, convenio o acuerdo con las terceras partes es propiedad del Aeropuerto Internacional Santa Ana.

RESPONSABILIDADES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Aeropuerto Internacional Santa Ana, cualquiera sea su situación, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe. Son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo. Las personas autorizadas a trabajar temporalmente deben cumplir estas normas, igualmente deben asumir las responsabilidades previamente dispuestas.

INCUMPLIMIENTO DE LA POLÍTICA.

La violación de la política será motivo para acciones disciplinarias incluyendo la terminación del contrato, acción civil y penal. El área de Recursos Humanos y/o Control Interno Disciplinario hará cumplir la respectiva sanción administrativa para los funcionarios que incurran en cualquiera de los siguientes delitos informáticos a través de Internet, los cuales pueden ser transfronterizos, así como analizar cómo afectaría a la Organización dichos sucesos:

- ✓ Acceso no autorizado.
- ✓ Destrucción de Datos o archivos o informes.
- ✓ Infracción de los derechos de autor.
- ✓ Infracción de Copyright de Bases de Datos.
- ✓ Interceptación de e-mail.
- ✓ Estafas electrónicas.
- ✓ Transferencias de Fondos en forma ilegal.
- ✓ Delitos convencionales como espionaje, terrorismo, narcotráfico, proselitismo de sectas, propaganda de grupos extremistas.
- ✓ Mal uso, como: Usos comerciales no éticos, agresión moral.
- ✓ Accesos a páginas de contenido no apto, o promueva el uso de éstas.
- ✓ Participar de juegos en línea a través de la red.

EXCEPCIONES.

Toda solicitud de excepción de alguna política debe ser solicitada previamente vía al Grupo de Tecnologías de la Información y las Comunicaciones y/o al gerente, con la debida justificación y documentación conforme a la naturaleza de su cargo o dado por eventos no declarados en las Políticas de Seguridad Informática; previa evaluación del alcance y el impacto. La evaluación de la excepción puede requerir el apoyo de la Oficina Jurídica y la Oficina Asesora de Planeación y/o Secretaría General.

Aprobada en Cartago, a los veinte (20) días del mes de diciembre de 2020.

ELABORO	REVISO	APROBO
CLAUDIA LIZETH VARGAS R. Contratista	**JUAN CARLOS ARIAS MONTOYA** Gerente	**JUAN CARLOS ARIAS MONTOYA** Gerente

JUAN CARLOS ARIAS MONTOYA
Gerente