ÍNDICE DE CONTENIDO

1. OBJETIVO

Establecer y dar a conocer las políticas generales del Sistema de Gestión de Seguridad de la Información en la Aerocivil como parte de la implementación de controles administrativos de seguridad de la información con el fin de incrementar la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

Estas políticas aplican para todos los procesos de la Entidad y las partes interesadas que acceden, almacenan, distribuyen y/o eliminan información de la Aerocivil.

3. GENERALIDADES

Este documento tiene la finalidad de describir las políticas del Sistema de Gestión de Seguridad de la Información de la Unidad Administrativa Especial de Aeronáutica Civil (Aerocivil), alineados a la Norma Técnica Colombiana NTC ISO 27001:2013, al Modelo de Seguridad y Privacidad de la Información de MINTIC (MSPI), a las normas nacionales e internacionales referentes a los mecanismos de protección de la confidencialidad, integridad y disponibilidad de la información aplicables a la Entidad.

La aplicación de las políticas de seguridad de la información debe proteger a la Entidad de cualquier amenaza que afecte la integridad, confidencialidad y disponibilidad de la información, aplicando los controles sobre; software, hardware, talento humano e infraestructura.

La seguridad de la información es un proceso de permanente evolución, debido a que las organizaciones enfrentan nuevas amenazas de acuerdo con su crecimiento y cambio de las condiciones de su entorno; por lo tanto, las políticas deben adaptarse a esta situación. Las políticas son documentos “vivos” que requieren una revisión y adaptación permanente, siempre con el visto bueno de la Alta Dirección.

Las políticas son la base de la gestión de la seguridad de la información y deben respaldar los objetivos estratégicos de la Entidad cumpliendo con los estándares y regulaciones aplicables. Las políticas permiten identificar los incumplimientos o desviaciones de los controles para cumplir con el ciclo de mejoramiento continuo PHVA (Planear – Hacer- Verificar- Actuar).

Las políticas están orientadas a minimizar los riesgos, incrementando la productividad con el uso aceptable de los activos de información bajo la perspectiva de controles que apoyen el cumplimiento de los objetivos organizacionales.

La actualización de las políticas no tiene un periodo definido, debe hacer parte del proceso de mejora continua en el cual se debe medir la eficacia de la gestión de la seguridad de la información y con base en esto decidir si las políticas deben ser actualizadas.

4. POLÍTICAS

A continuación, se establecen las políticas de seguridad de la información, las cuales dan las directrices de alto nivel en cuanto a la instauración de los controles administrativos del SGSI (Sistema de Gestión de Seguridad de la Información).

4.1 Administración de Cambios

Los cambios son responsabilidad del propietario de la información o líder del proceso y deben cumplir con la debida diligencia para que los recursos necesarios estén disponibles. Los lineamientos son:

- Para la aprobación de los cambios se debe incluir en sus requerimientos un análisis de riesgos de seguridad de la información y los controles definidos para mantener estos riesgos en un nivel aceptable acorde con la Guía de Gestión de Riesgos de Seguridad de la Información.
- Todo cambio que afecte componentes tecnológicos debe ser aprobado formalmente por el propietario de la información afectada, el administrador del Componente Tecnológico, el Coordinador del Grupo Soporte Informático y el Director de Informática.
- Todo cambio en los Sistemas de Información debe ser probado y ejecutado en un ambiente de desarrollo y pruebas antes de ser implantado en el ambiente de producción. En todos los cambios los roles de pruebas, validación de las pruebas, certificación y puesta en producción deben ser de colaboradores diferentes.
- Para la administración de cambios se debe aplicar el procedimiento correspondiente definido por la Aerocivil, de acuerdo con el tipo de cambio solicitado en el Componente Tecnológico.
- Cualquier cambio en Componentes Tecnológicos debe quedar formalmente documentado desde su solicitud hasta su implantación incluyendo el análisis de impacto del cambio realizado; este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

4.2 Auditoria de Seguridad de la Información

Se deben establecer mecanismos para verificar y evaluar el cumplimiento de las políticas, procedimientos y estándares definidos en el MSPI. Los lineamientos de esta política son:

- Se debe realizar una auditoría interna al SGSI, al menos una vez por año, generando los informes requeridos para el ciclo de mejoramiento continuo, establecido en el MSPI.
- Las auditorías de seguridad de la información deben regirse por el plan de auditorías anuales de la Aerocivil.
- Durante la ejecución de la auditoria debe realizarse acompañamiento constante por el colaborador asignado por la Aerocivil.
- El Grupo de Seguridad de la Información debe apoyar las auditorías realizadas al SGSI sin intervenir en la independencia de los auditores en sus observaciones.

- Se deben crear cuentas especiales para auditoria en los sistemas de información y aplicaciones, en el alcance, con permisos de solo lectura.
- Se debe proporcionar acceso a los auditores a las zonas de trabajo (oficinas, cubículos, áreas de almacenamiento, entre otros).
- Se debe contar con disponibilidad para la atención de los auditores durante la ejecución de la auditoria.
- El desarrollo de las auditorias debe contemplar que las acciones correctivas pueden generar planes de mejoramiento, que requieren inversiones acordes con la criticidad de los hallazgos.
- Se deben tener configurados registros en los sistemas de información que cubran los siguientes aspectos:

    - Modificación de configuración de seguridad.
    - Creación, modificación o eliminación de cuentas de usuario.
    - Creación, modificación y eliminación de registros de auditoría.
    - Creación, modificación y eliminación de activos de información

4.3 Capacitación y Toma de Conciencia

Las "personas" son el factor más importante para lograr la seguridad de la información por tanto se establecen las siguientes directrices:

- Todos los colaboradores deben ser capacitados en las políticas y procedimientos de seguridad de la información, así como en el marco legal y regulatorio aplicable.
- Desarrollar las habilidades y capacidades para el manejo de herramientas de seguridad informática, incluyendo la detección de anomalías a ser reportadas.
- Se deben ejecutar campañas periódicas, al menos una vez por año, en las que se busque la continua toma de conciencia de los colaboradores de la Entidad con la seguridad de la información.
- El Grupo de Seguridad de la Información es responsable por la definición de los contenidos de los programas de formación en este campo, la Dirección de Talento Humano se responsabiliza por su ejecución y evaluación.
- Todos los colaboradores deben aprobar la evaluación sobre los aspectos de seguridad de la información exigidos de acuerdo con los roles y responsabilidades definidos.

4.4 Comunicaciones Digitales

Alineándose con la política de Gobierno Digital, la Aerocivil da preponderancia a las comunicaciones digitales sobre las demás formas existentes, para esto se deben aplicar los siguientes lineamientos:

- El propietario de la información debe definir dentro del uso aceptable, la forma en que es permitida la comunicación digital, señalando cuando sea necesario el uso de controles criptográficos para proteger la confidencialidad y la integridad.
- Se debe implementar la trazabilidad de las comunicaciones digitales, garantizando las evidencias necesarias para la gestión de incidentes, auditorías o solicitudes de entes de control.

- El uso de las comunicaciones digitales debe estar plenamente justificado por las labores asignadas al cargo del responsable correspondiente. La validación de los contenidos que incumplan esta política es una actividad del Grupo de Soporte Informático y la evaluación y medidas correspondientes son responsabilidad de la Dirección de Talento Humano.
- El intercambio de información por este medio debe estar estrictamente ajustado a lo que establezca la política de control de acceso de la información involucrada.
- Se debe guardar el registro digital de las comunicaciones digitales de acuerdo con lo establecido en el Marco Legal y Regulatorio Colombiano.
- No se debe guardar un registro impreso de las comunicaciones digitales.
- Cualquier tipo de comunicación digital debe ser firmada por el colaborador que la origina.
- Los usuarios son responsables de la validación del contenido de los mensajes recibidos y deben abstenerse de la ejecución o uso de los archivos adjuntos cuando no cumplan con el estándar de comunicaciones digitales.
- Las comunicaciones digitales pueden ser objeto de monitoreo por efectos de gestión de riesgos de seguridad de la información.
- Los servicios de comunicaciones digitales (correo electrónico, mensajería instantánea, redes sociales, herramientas colaborativas) deben ser utilizados con cuentas de usuario asignados en forma personal e intransferible a cada colaborador, siguiendo los estándares de comunicaciones digitales.
- Cuando se requiera el uso compartido de una cuenta, se deberá implementar un mecanismo que enmascare con un nombre identificativo común (MSPI, Misión-SI, Aerosanito) manteniendo la trazabilidad de los colaboradores en forma independiente. En ningún caso se acepta compartir cuentas de usuario por dos o más colaboradores.
- Cada colaborador se hace responsable del manejo del software cliente asignado (buzón de correo, cliente de mensajería instantánea, software para herramientas colaborativas) para el servicio de comunicaciones correspondiente.
- Se debe propender por el envío de enlaces de acceso en lugar de archivos; también se debe enviar las comunicaciones a los destinos estrictamente necesarios. Esto con el fin de no ocupar inapropiadamente los recursos informáticos.
- Las comunicaciones digitales para asuntos personales deben estar autorizadas por el Jefe Inmediato cumpliendo con el estándar para comunicaciones digitales.

4.5 Confidencialidad

Para toda la información que esté bajo la responsabilidad de la Aerocivil se establece que debe aplicarse los mecanismos de protección de la confidencialidad de la siguiente forma:

- Para los activos de información con clasificación alta y media para la confidencialidad y que tengan que ser enviados por fuera de la Aerocivil, deben ser cifrados con un algoritmo criptográfico fuerte.
- Todos los privilegios de acceso para los activos de información con niveles de confidencialidad alta y media deben ser restringidos a los que aprueba el propietario de la información y que estén formalmente caracterizados en el proceso correspondiente.

- La información clasificada en los niveles de confidencialidad alto y medio solo puede ser almacenada en forma cifrada en servidores de almacenamiento autorizados por el propietario y que cumplan con la política de control de acceso correspondiente.

4.6 Continuidad de la Seguridad de la Información

El Sistema de Gestión de Continuidad de Negocio es paralelo e independiente al Sistema de Gestión de Seguridad de la Información, dentro del MSPI se deben implementar los mecanismos para que los controles definidos para proteger la confidencialidad, integridad y disponibilidad de la información se mantengan cuando se activen las estrategias de continuidad y esto se logra a través de los siguientes lineamientos:

- Los controles criptográficos para proteger la confidencialidad y la integridad deben ser implementados en las copias de respaldo y los sistemas redundantes.
- El registro de acciones y operaciones debe mantenerse bajo las mismas condiciones de los sistemas principales en los sistemas redundantes, que se activen en caso de una contingencia.
- El control de acceso debe mantener las restricciones y privilegios en los sistemas redundantes y para las copias de respaldo, acorde con lo establecido por el propietario de la información.

4.7 Control de Acceso

Los propietarios de la información o líderes de los procesos son los responsables de la definición de los requisitos para el acceso a la información y de sus restricciones tanto en el entorno físico como en el digital. El acceso a la información debe ser autorizado con base en el principio del mínimo privilegio posible, esto es, que se entrega a cada colaborador lo estrictamente necesario para el desempeño de sus funciones y con esto adquiere el rol de custodio de la información. Las directrices de esta política son:

4.7.1 Generales

- Se debe deshabilitar o eliminar los usuarios correspondientes al personal cuya relación contractual con la Aerocivil haya finalizado.
- Para la eliminación y creación de usuarios se debe seguir el Procedimiento de Ingreso y Vinculación de Personal.
- Para conceder acceso a cada sistema de información de la Aerocivil, se debe asignar una cuenta de usuario única a cada persona o aplicación autorizada para ingresar a dicho sistema.
- Para generar tanto acceso físico como lógico a proveedores y contratistas, el supervisor del contrato o su superior inmediato, debe realizar la solicitud al propietario de la información.
- Una vez que la relación contractual del contratista o proveedor haya finalizado, el supervisor del contrato o su superior inmediato, es responsable de solicitar,

inmediatamente, la eliminación de los derechos de acceso a el(los) usuario(s) relacionado(s) con ese contrato.

- Una vez se presente un cambio de cargo para un servidor público o un modificatorio del contrato a un contratista, el jefe inmediato o supervisor del contrato es responsable de solicitar, inmediatamente, la actualización de los derechos de acceso al usuario relacionado.
- La vigencia de cualquier cuenta asociada a un contrato debe ser la que establezca la duración de las actividades correspondientes a esa cuenta en las especificaciones del contrato. El supervisor del Contrato es responsable por el reporte de las novedades en el contrato para que las cuentas sean retiradas o reemplazadas acorde con las situaciones que se presenten.
- La definición del tiempo de vigencia de las cuentas de usuario de los servidores públicos con vinculación laboral directa con la Aerocivil es responsabilidad del Jefe Inmediato.
- Aquellas cuentas de usuario que se encuentran en periodo de hibernación (cuentas deshabilitadas, pero no eliminadas), deben eliminarse del todo en un máximo de 6 (seis) meses.
- Cada colaborador de la Aerocivil debe responsabilizarse de los usuarios y claves que le son asignados para el acceso a los recursos de la plataforma tecnológica, los servicios de red y los sistemas de información de la Entidad.
- Los colaboradores de la Aerocivil por ninguna circunstancia deben compartir sus cuentas de usuario y claves con otras personas.
- Se deben realizar revisiones periódicas, de mínimo una vez al mes, en los sistemas de información de la Aerocivil para que se pueda verificar que se han removido los usuarios deshabilitados, y que los derechos de acceso que hayan caducado no se encuentren activos.
- El tiempo máximo permitido sin uso de una cuenta de usuario, es de 2 meses, después de este período la cuenta entrará en hibernación.

4.7.2 Administración de acceso lógico

- La especificación de los accesos y perfiles en los servicios de red, aplicaciones y sistemas de información es responsabilidad del líder del proceso al que pertenece la cuenta de usuario.
- Se deben generar mecanismos de trazabilidad a los encargados de la administración del acceso a los sistemas de información, los servicios de red y a los recursos de la plataforma tecnológica.
- Los administradores de los sistemas de información o aplicaciones deben crear, eliminar, modificar o bloquear las cuentas de los usuarios únicamente con la autorización de la Dirección de Talento Humano para los servidores públicos vinculados directamente a la Entidad o del área responsable que aplique para los demás colaboradores.
- El jefe inmediato de cada colaborador o el administrador del contrato que aplique son los únicos autorizados para solicitar a la Dirección de Talento Humano, novedades sobre las cuentas de usuario.
- El propietario del activo de información debe especificar los permisos de acceso con base en perfiles de usuario, en ningún caso directamente sobre personas.

- Los ambientes de desarrollo, pruebas y producción deben estar en entornos de red independientes.
- Se deben establecer controles de acceso a los ambientes de desarrollo, pruebas y producción.
- Se deben habilitar los registros de auditoria de administración que brinden información sobre la creación de usuarios y cambios de políticas de seguridad del sistema.

4.7.3 Administración de acceso físico

- Todos los colaboradores de la Aerocivil deben portar el carné en un lugar visible mientras se encuentren en las instalaciones de la Entidad.
- Una vez que un colaborador finalice su vínculo contractual con la Entidad, se deben bloquear los privilegios de acceso físico a las instalaciones de la Aerocivil, y de igual forma se debe realizar la devolución del carné institucional.
- Todos los visitantes que ingresen a las instalaciones de la Aerocivil deben portar una identificación en un lugar visible mientras se encuentren en la Entidad.
- Se debe identificar a todo el personal que requiere acceso a las instalaciones físicas de la Aerocivil, de igual manera, se requiere autorizar el ingreso y conceder privilegios acordes al rol de cada colaborador o visitante.
- Toda persona que ingrese al centro de cómputo se debe registrar en una bitácora, la cual debe estar ubicada a la entrada en un lugar visible.
- El ingreso al centro de cómputo debe ser monitoreado permanentemente, con el fin de identificar el acceso no autorizado.
- Deben permanecer cerradas y aseguradas todas las puertas de acceso de las áreas que custodien información Pública Clasificada y/o Pública Reservada.
- Se debe tener controles de acceso para las áreas seguras de la Aerocivil (Oficina de Control Interno, centro de cómputo y demás oficinas que custodien información Pública Clasificada o Pública Reservada); por ejemplo: puertas de seguridad, sistemas de control con lectores biométricos, cámaras de vigilancia, sistema de alarmas, archivadores bajo llave, entre otras, que el análisis de riesgos y su plan de tratamiento determine necesarios.
- Para el acceso físico a las instalaciones de la Entidad, debe seguirse el Procedimiento de Control de Acceso Físico.

4.8 Controles Criptográficos

Se debe hacer uso de algoritmos criptográficos fuertes, es decir para los que a la fecha no se tengan vulnerabilidades para proteger la confidencialidad e integridad de la información; todas las partes interesadas en el alcance deben cumplir las siguientes directrices:

- El uso de controles criptográficos únicamente es válido cuando sea el resultado de un análisis de riesgos y su implementación sea autorizada por el propietario de la información correspondiente.
- Se debe cifrar en almacenamiento y en tránsito toda la información catalogada como clasificada o reservada.

- Las contraseñas de acceso a los sistemas de información solo pueden almacenarse o transmitirse con el uso de controles criptográficos.
- Se debe firmar digitalmente la información con nivel de clasificación Alto para Integridad.
- Para realizar la distribución de la contraseña de cifrado de un archivo, esta debe hacerse a través de un medio diferente al del envío de este.
- Por defecto, se hará uso de algoritmos de cifrado asimétrico y se permitirá el uso de algoritmos de cifrado simétrico solo para VPNs.

4.9 Copias de Respaldo

Los propietarios de la información deben mantener actualizado el Análisis de Impacto de Negocio (BIA) y sobre sobre esta base definir las estrategias de recuperación, dentro de las cuales se establece los requerimientos para las copias de respaldo.

Con la claridad por parte de los propietarios de la información para las copias de respaldo, la Dirección de Informática debe implementar las soluciones que atiendan estos requerimientos y que serán aplicables para equipos de usuario y servidores. Los lineamientos de esta política son:

- La responsabilidad de la ejecución de las copias de respaldo es del custodio designado por parte del propietario. Este custodio puede ser el Grupo de Soporte Informático, una compañía contratada externamente o a quien el propietario designe.
- El propietario de la información debe garantizar que la ejecución de las copias de respaldo sea asignada acorde con los requerimientos definidos.
- Quien sea designado como responsable de la copia de seguridad debe mantener actualizada la tecnología requerida para la copia y restauración, previniendo riesgos asociados con la obsolescencia tecnológica.
- Las copias de respaldo deben mantener los controles criptográficos de la información original.
- Solo se realizan copias de respaldo de los activos de información que previamente hayan sido identificados y valorados acorde con la Metodología de Gestión de Activos de Información.
- Se debe contar con una matriz de información de las copias de respaldo, ejecutadas en la Entidad con datos sobre el tipo de contenido, la frecuencia de ejecución, los medios de almacenamiento, tiempo de almacenamiento y borrado de esta información.
- Los medios de respaldo deben ubicarse en un lugar que cuente con acceso restringido y con las condiciones ambientales necesarias para su conservación acorde a lo especificado por el fabricante.
- Todo dispositivo de almacenamiento debe ser etiquetado acorde al nivel de clasificación de la información que allí contenga.
- Se debe tener registro de la ejecución de las copias de respaldo, al igual que de la restauración de estas.
- Se deben realizar pruebas aleatorias respecto a la restauración de las copias de respaldo de forma controlada y en un ambiente controlado que contenga los mismos niveles de seguridad del ambiente original.

- Se debe dejar registro de la ejecución de las pruebas de restauración de copias de respaldo.

4.10 Cumplimiento

La Aerocivil debe cumplir con los requisitos legales internos y externos aplicables a la Seguridad y Privacidad de la Información, tales como: Ley de Delitos Informáticos, Ley de Transparencia, Ley de Derechos de Autor, Ley de Protección de Datos Personales, los tiempos de retención de registros, el uso autorizado de recursos de procesamiento, el uso de algoritmos criptográficos fuertes, la recolección de evidencias y la realización de auditorías.

La Aerocivil, de conformidad con la legislación vigente en materia de responsabilidad civil, penal, administrativa, disciplinaria y en especial de las normas contenidas en la Ley 734 de 2002, aplica las medidas correspondientes, cuando una persona natural o jurídica viole la normatividad del Modelo de Seguridad y Privacidad de la Información, por omisión, extralimitación o intencionalmente.

4.11 Derechos de Autor

Se debe aplicar la Ley de Protección de Derechos de Autor para todos los documentos y software utilizado por la Aerocivil. Se debe cumplir con los siguientes aspectos:

- Esta política aplica para los documentos impresos, digitales o en un medio análogo.
- Se deben identificar los derechos de uso de cualquier documento que sea requerido por la Aerocivil y cumplir estrictamente lo que el autor o titular de los derechos patrimoniales establezca.
- La copia de un documento únicamente puede llevarse a cabo si es un documento público o si se adquirió el derecho para esta acción, teniendo claro que el valor es proporcional al número de copias que se generen.
- Todos los documentos bajo la responsabilidad de la Aerocivil deben cumplir con el etiquetado de activos de información definido en la Metodología de Gestión de Activos de Información y así facilitar la identificación de la restricción de acceso que aplique.
- La publicación de documentos en cualquier medio por parte de la Aerocivil es permitida únicamente para los activos de información de tipo “Público”.
- Todo el software que se utilice en la Aerocivil debe este licenciado, esto es independiente de cualquier condición es decir aplica si el software es comercial o gratuito, abierto o cerrado, si es para un servidor o para un computador de usuario, si está en demostración o en uso.
- Se debe tener claro que el licenciamiento de un software no se limita al pago de los derechos patrimoniales sino también a las condiciones de uso y las exigencias que el autor pueda hacer en los términos existentes.
- Todo el software que se adquiera o use en la Aerocivil debe cumplir con los Procedimientos de Adquisición y uso de Software Original y de Verificación de los requisitos legislativos y normativos relacionados con los derechos de propiedad intelectual.
- Los Líderes de los procesos deben estimar dentro de sus presupuestos los costos relacionados con el licenciamiento de uso de software y documentos.

4.12 Desarrollo Seguro

Los líderes de los procesos deben cumplir con la gestión para que se definan los requerimientos funcionales y no funcionales del software. Dentro de los requerimientos no funcionales se encuentran los de seguridad de la información que se deben establecer de acuerdo con los resultados del análisis de riesgos. La Dirección de Informática es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con desarrollos, actualizaciones e instalaciones de software y planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los entornos de producción. Los lineamientos de esta política son:

- Para el desarrollo de aplicaciones debe seguirse el Procedimiento de desarrollo y mantenimiento de Software.
- Se debe generar un acuerdo previo con desarrolladores y fábricas de software, el cual debe establecer la protección de la propiedad intelectual y la confidencialidad de la información gestionada en los proyectos de desarrollo.
- Se debe definir y estandarizar el ciclo de vida y los criterios de desarrollo seguro, aplicando las buenas prácticas y lineamientos para restricciones de captura de datos, definición de variables y manejo de excepciones.
- La documentación de los desarrollos debe generarse durante el ciclo de vida de desarrollo, debe ser revisada por los usuarios finales, actualizarse si cambia alguna de las funcionalidades y almacenarse en un servidor administrado por la Dirección de Informática de la Aerocivil.
- Cualquier cambio que se ejecute durante el ciclo de vida de desarrollo, debe pasar por un control de cambios en donde se evalúen los riesgos de seguridad de la información.
- Todo software o sus modificaciones deben ser analizados previamente en un ambiente de pruebas independiente para la identificación de vulnerabilidades de seguridad de la información. Las pruebas deben ser documentadas y deben contar con la aprobación del propietario de la información para el paso a producción.
- Los datos de prueba utilizados no deben hacer uso de información de producción.
- Se debe elaborar una guía detallada del paso a producción, definiendo los recursos requeridos, contingencias, chequeos en cada paso cumplido y criterios de aceptación del cambio.
- Los desarrolladores no deben tener acceso a los entornos de producción.
- Todo sistema desarrollado por la Aerocivil debe generar el protocolo de las condiciones de autenticación a la aplicación, el cual debe ser revisado y aprobado por el Grupo de Seguridad de la Información.
- Se deben incluir las opciones de autenticación de acuerdo con los requerimientos de seguridad de la información, esto incluye los factores adicionales al de usuario y contraseña como son: tokens de seguridad, controles biométricos y contraseñas de un solo uso enviadas al dispositivo móvil.
- No permitir la ejecución de comandos del sistema operativo desde el software desarrollado o adquirido.

- Garantizar que el software en su funcionamiento e inclusive en situaciones de excepción, anormales o de falla nunca entregue información clasificada o reservada (especificaciones de la tecnología utilizada, direcciones IP, rutas de acceso, nombres de archivos, nombres y versiones de aplicaciones de software, código fuente, información de errores y cadenas de conexión).
- Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.
- Establecer la identificación de vulnerabilidades técnicas para todas las librerías y demás componentes utilizados en el desarrollo de software.
- No se deben dejar en comentarios o quemadas en el código del software las credenciales de acceso o autenticación.
- Los comentarios escritos por los desarrolladores en el programa fuente no deben divulgar innecesariamente la información de configuración.
- No se deben dejar quemadas en el código direcciones IP o nombres de máquinas, estas deben poderse cambiar directamente en la configuración del software.
- Crear la funcionalidad para que se asegure el cierre de las sesiones por desuso o tiempo de conexión de acuerdo los requerimientos de seguridad.

4.13 Dispositivos Móviles

Son catalogados como dispositivos móviles: Los computadores portátiles, teléfonos móviles y tabletas requeridos por los colaboradores de la Entidad y es el propietario de la información quien define los activos de información que se permiten manejar en estos dispositivos. Se debe validar con el Grupo de Soporte Informático la instalación o configuración de los controles para contar con la protección acorde con las políticas de seguridad de la información. Las directrices de la política son:

- En los dispositivos móviles se debe cumplir con la Política de Control de Acceso correspondiente a la información que maneje.
- La instalación de software en dispositivos móviles debe cumplir con la Política de Hardware y Software de la Aerocivil.
- La seguridad física del dispositivo móvil es responsabilidad del usuario que lo tiene asignado, este debe cumplir con los procedimientos y estándares del MSPI.
- Aceptar y permitir que la información de la Entidad almacenada en el dispositivo móvil puede borrarse de forma remota si el dispositivo es afectado por un incidente de seguridad de la información o si el responsable del dispositivo termina su relación contractual con la Aerocivil.
- El usuario del dispositivo móvil debe aceptar la instalación de los controles de seguridad y estas no podrán ser modificadas mientras se acceda o almacene información de la Aerocivil.
- Instalar y configurar las herramientas de antimalware con las que cuente la Entidad.
- Implementar en el dispositivo móvil los controles criptográficos exigidos para los activos de información que maneje.

- Para los dispositivos que son propiedad de la Aerocivil está prohibido ejecutar volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.
- Se prohíbe la modificación o desactivación de las configuraciones realizadas por la Aerocivil en el dispositivo móvil para el uso de redes públicas, debe garantizarse una conexión cumpliendo con los requerimientos de seguridad de los activos de información manejados.
- Establecer una lista blanca de aplicaciones que son permitidas en los dispositivos móviles.
- No es permitido almacenar en dispositivos móviles datos catalogados como reservados o clasificados.
- Se deben definir los tipos de dispositivos, tecnologías, sistemas operativos y versiones de dispositivos móviles que se permiten conectar a la red corporativa de datos de la Entidad.
- No se debe permitir la conexión a la red corporativa de datos de la Entidad, de dispositivos móviles que no cumplan con los controles de seguridad informática definidos en el MSPI.
- En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la Aerocivil, se debe seguir el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

4.14 Documentación

Se debe mantener documentación actualizada y con el formato definido por el Sistema de Gestión de la Aerocivil, aplicando los siguientes lineamientos:

- Todos los procedimientos relacionados con procesamiento digital de información deben estar documentados con el nivel de detalle necesario para que una persona nueva en el cargo pueda proceder en forma autónoma.
- Toda la documentación de procesamiento digital debe mantenerse en este formato, no se permite el uso impreso de esta información.
- Se debe determinar con el apoyo del Grupo Seguridad de la Información y la Oficina Asesora Jurídica cuales de los documentos podrían pertenecer al nivel clasificado y reservado, para que se restrinja su acceso y se mantenga la trazabilidad sobre su uso, es fundamental establecer la verificación de integridad de este tipo de documentos, es suficiente con el uso de algoritmos de hashing.

4.15 Escritorio y Pantalla Limpia

Se debe proteger la información impresa, almacenada en medios removibles y visible en la pantalla de los equipos informáticos para que su acceso solo sea permitido a las personas autorizadas de acuerdo con la Política de Control de Acceso. Los lineamientos definidos son:

- Mantener los documentos y medios de almacenamiento removibles en los lugares destinados para este propósito como son escritorios, archivadores y demás que apliquen. Estos elementos solo pueden estar por fuera de estos sitios cuando estén siendo usados por la persona autorizada, una vez termine la actividad se debe guardar inmediatamente.
- La impresión de documentos con información Clasificada o Reservada solo se debe permitir cuando el Propietario correspondiente lo haya autorizado. Con esta autorización una vez se

imprima debe retirarse el documento en forma inmediata del equipo destinado para esta tarea.

- Bloquear la pantalla del equipo de cómputo cada vez que el usuario no se encuentre trabajando sobre este.
- Todos los equipos de cómputo deben tener configurado el cierre automático de sesión por inactividad; el tiempo será determinado por cada propietario de la información o líder de proceso.
- Organizar la información en el escritorio virtual para prevenir la visualización de información clasificada o reservada.

4.16 Gestión de Activos de Información

Esta gestión es responsabilidad de todos los colaboradores de la Aerocivil y se debe cumplir aplicando la Metodología de Gestión de Activos de Información aprobada por la Entidad. Las directrices son:

- Toda la información manejada por los colaboradores de la Entidad en el desempeño de sus funciones debe estar registrada en el Inventario de Activos de Información.
- Es responsabilidad del propietario del activo de información, su actualización y mantenimiento.
- Es responsabilidad del propietario del activo de información, la definición del uso aceptable que consiste en la forma como se restringe o permite su uso; esto determina donde puede ser almacenado, si se permite el uso de medios removibles, si puede o no ser impreso, si se debe firmar digitalmente, el registro para las operaciones aplicadas (creación, consulta, copia, modificación, eliminación), si se debe cifrar y los privilegios para todo su ciclo de vida.
- Se debe realizar al menos, una revisión anual al inventario de activos de información.
- Se debe seguir la Metodología de gestión y clasificación de activos de información y el Instrumento para el diligenciamiento de la matriz de activos de información.
- Los propietarios de la información deben cumplir con la gestión requerida para que se cumpla el etiquetado de los datos en todas sus instancias identificando el nivel de clasificación frente a la confidencialidad, integridad y disponibilidad establecida en el Inventario de Activos de Información.
- El propietario de la información debe definir los procedimientos para controlar y dejar evidencia del ciclo de vida de cada activo de información estableciendo claramente las actividades y sus responsables para la creación, modificación, eliminación, asignación y devolución de cada activo.

4.17 Gestión de Incidentes de Seguridad de la Información

Garantizar que cualquier evento que pueda afectar la integridad, confidencialidad o disponibilidad de la información, sea identificado oportunamente, reportado y tratado de acuerdo con la criticidad que pueda representar para la Aerocivil, de tal manera que se evite o se minimice los daños para la Entidad y que haya un aprendizaje para que se prevenga su recurrencia.

- Para la gestión de incidentes se debe seguir paso a paso el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Los eventos de seguridad de la información se registran a través de la mesa de servicio de la Dirección Informática y en esta se analizarán y registrarán las acciones ejecutadas durante la investigación y mitigación del incidente.
- Se considera un evento de seguridad de la información, cualquier situación relacionada con el incumplimiento de las políticas, procedimientos o estándares de seguridad de la información.
- La mesa de servicio es responsable por el registro, valoración y escalamiento de todos los eventos de seguridad de la información reportados.
- El escalamiento debe hacerse al técnico responsable de su tratamiento y al propietario de la información afectado.
- El registro de los eventos de seguridad de la información debe hacerse en el Sistema de Información designado para este propósito y estar soportado por las comunicaciones o el correo electrónico corporativo enviado al colaborador que reportó el incidente, al responsable de su tratamiento y al propietario de la información afectado.
- Un evento de seguridad de la información se cataloga como incidente o como un falso positivo de acuerdo con establecido en el Procedimiento de Gestión de Incidentes. La mesa de servicio debe hacer el seguimiento respectivo para el tratamiento que aplique en cada caso.
- El propietario de la información afectada por un incidente es el responsable por el contacto con las autoridades cuando el incidente de seguridad así lo amerite.
- El propietario de la información debe proceder con la gestión de riesgos de seguridad de la información que aplique, una vez se declare un incidente que afecte un activo bajo su responsabilidad.
- El propietario del activo información afectado por un incidente es el responsable por la gestión requerida para el proceso de aprendizaje en la Aerocivil que evite la recurrencia de ese tipo de situaciones. Para esto debe contar con la participación activa de los procesos de soporte que aplique como son: Gestión de las Tecnologías de la Información, Gestión de Talento Humano y Gestión de bienes y servicios.

4.18 Gestión de Llaves Criptográficas

Proteger la confidencialidad, integridad y disponibilidad de las llaves criptográficas aplicando las siguientes directrices:

- Las llaves criptográficas deben ser almacenadas en forma cifrada, cumpliendo con la Política de Control Acceso.
- Hacer uso del Procedimiento de Gestión de Llaves Criptográficas
- Cada vez que sea activada una llave criptográfica será asignada a un colaborador que se convierte en Custodio de este activo de información y por ningún motivo puede compartir o delegar su uso.
- La solicitud de llaves criptográficas debe realizarse formalmente a través de la Mesa de servicio de la Dirección de Informática.

- Se debe mantener el registro de todas las operaciones con las llaves criptográficas, como son: creación, asignación, activación, desactivación y eliminación.
- Si las llaves se almacenan en medios extraíbles, el responsable asignado debe garantizar su custodia permanente cuando no se encuentren en el medio destinado para su almacenamiento.
- Las llaves solo pueden almacenarse en servidores o computadores de usuario autorizados para este propósito.
- Cuando se considere que una llave puede estar comprometida por acceso no autorizado, se debe iniciar el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- La revocación de las llaves es responsabilidad del Grupo de Soporte Informático y esto se lleva a cabo cuando se concluya que es la acción a seguir como parte del tratamiento de un incidente de seguridad de la información acorde con las Políticas de Seguridad de la Información.
- El cambio o actualización de las llaves debe ser solicitado por el jefe del custodio.

4.19 Hardware y Software

El hardware y software se convierten en la herramienta de trabajo más importante para la Aerocivil y su uso se debe hacer de acuerdo con los siguientes lineamientos:

- El software que se use para la Aerocivil debe estar explícitamente aprobado por el Líder del Proceso.
- La instalación de software sin contar con la autorización del Líder del Proceso y que no tenga el licenciamiento acorde con el Marco Legal y Regulatorio Colombiano, conlleva a un proceso disciplinario.
- Todo el software debe ser adquirido aplicando el Procedimiento para asegurar la adquisición o uso de software original.
- Quien asuma el rol de responsable del software debe cumplir con la debida diligencia para que se garantice el licenciamiento requerido, soporte especializado permanente, mantenimiento y gestión de vulnerabilidades acorde con los requerimientos de seguridad de la información del proceso correspondiente.
- Todo el software instalado en la Aerocivil debe contar con un contrato de soporte que incluya el reporte de las vulnerabilidades acorde con las amenazas cibernéticas a nivel global. El propietario del software debe garantizar los recursos para que las vulnerabilidades reportadas sean remediadas oportunamente para prevenir daños a los intereses de la Aerocivil.
- Todo software instalado en la Aerocivil debe contar con un servicio de detección proactiva de vulnerabilidades con soluciones automatizadas que hagan uso de técnicas acordes con las amenazas cibernéticas a nivel global.
- El responsable del software debe definir los requerimientos de seguridad aplicando la guía de gestión de riesgos de la Entidad.
- Todo proveedor de software debe garantizar contractualmente el soporte para la solución de las vulnerabilidades identificadas. Este soporte debe incluir la generación de versiones que corrijan las vulnerabilidades identificadas, complementado con una asesoría para lograr protección con soluciones de seguridad perimetral.

- La Dirección de Informática únicamente puede implementar los requerimientos de seguridad que el responsable del software haya autorizado.
- La Dirección de Informática y las áreas responsables de TI en la Entidad son las únicas áreas autorizadas para instalar, desinstalar, configurar, probar, activar o inactivar en producción cualquier tipo de software.
- La Dirección de Informática y las áreas responsables de TI en la Entidad son las únicas áreas autorizadas para instalar, desinstalar, configurar, probar, activar o inactivar en producción cualquier tipo de hardware.
- La adquisición del hardware debe estar autorizado por la Dirección de Informática y las áreas responsables de TI en la Entidad.
- Todo el hardware utilizado en la Aerocivil debe responder específicamente a las necesidades del software autorizado.
- La Dirección de Informática debe reportar a los propietarios de información correspondiente de la tecnología que administra, los tiempos de obsolescencia para que se tomen las medidas oportunas para la actualización del software y hardware requeridos.
- El uso de software o hardware que no esté explícitamente autorizado debe tratarse aplicando el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- La disposición de hardware debe contar con un procedimiento de borrado seguro de la información, el cual debe ser solicitado por los propietarios de la información y ejecutado por el Grupo de Soporte Informático.

4.20 Integridad

Para toda la información que esté bajo la responsabilidad de la Aerocivil se establece que deben aplicarse los mecanismos de verificación de integridad de la siguiente forma:

- Para los activos de información con clasificación alta para la Integridad y que tengan que ser enviados al exterior de la Aerocivil o publicados en el portal deben ser protegidos con firma digital.
- Todas las modificaciones para los activos de información clasificados con niveles de Integridad alta y media deben ser registrados y monitoreados.
- Todos los privilegios de modificación para los activos de información con niveles de integridad alta y media deben ser restringidos a los que apruebe el propietario de la información y que estén formalmente caracterizados en su proceso.
- Las modificaciones a los activos de información con niveles de integridad alta y media no pueden realizarse en computadores de usuario, únicamente en los servidores aprobados formalmente por el propietario de la información y formalmente caracterizados en su proceso.

4.21 No Repudio

Para toda la información que este bajo la responsabilidad de la Aerocivil se establece que deben aplicarse los mecanismos de registro para tener evidencia suficiente sobre la copia o consulta de información en los niveles medio y alto para confidencialidad, la modificación sobre información

con nivel alto para integridad y el borrado o cambio de ubicación para la información con nivel alto para disponibilidad. En cada caso se debe guardar el registro y garantizar las condiciones para endilgar la responsabilidad a la persona que ejecutó la acción correspondiente y contar con los registros que tengan la validez dentro del Marco Legal y Regulatorio Colombiano. De la misma forma se debe adaptar el proceso disciplinario para que sean aplicadas las sanciones para el incumplimiento de las políticas de seguridad sobre la base de las evidencias citadas en este lineamiento.

4.22 Procesamiento Digital

Alineándose con la política de Gobierno Digital, la Aerocivil da preponderancia al procesamiento digital sobre el manual o impreso, para esto se deben aplicar los siguientes lineamientos:

- El propietario de la información solo debe permitir la impresión de documentos cuando esto sea estrictamente necesario, la tendencia debe ser el procesamiento digital.
- Se debe hacer uso de algoritmos de cifrado fuertes para garantizar la confidencialidad de la información reservada y clasificada.
- Se debe hacer uso de firmas digitales para la protección de la información clasificada en nivel alto de integridad.
- Se debe implementar la trazabilidad de las acciones de los usuarios sobre el ciclo de vida de cada activo de información.
- El control de acceso a la información debe hacerse de acuerdo con las restricciones y privilegios definidos por el propietario de la información y se debe guardar un registro detallado de todas las novedades sobre las cuentas de usuario.
- El reloj de cualquier dispositivo conectado a la red corporativa de datos de la Entidad debe estar sincronizado con el servidor NTP.

4.23 Propiedad de la Información

Se establece en la Aerocivil el rol de propietario de la información que tiene bajo su responsabilidad los siguientes aspectos:

- Que la información se encuentre actualizada en el inventario de activos de información, cumpliendo con la Metodología de Gestión de Activos de Información de la Entidad.
- Gestionar el presupuesto requerido para que la información cuente con los controles definidos de acuerdo con el análisis de riesgos de seguridad de la información.
- Cumplir con la debida diligencia para que el plan de tratamiento de riesgos que cubra la información bajo su responsabilidad se cumpla oportunamente.
- Definir las restricciones y privilegios de acceso para la información aplicando el principio del mínimo privilegio posible; debe contar con los mecanismos de reporte de anomalías para que se tomen las acciones correctivas oportunas.

4.24 Relación con Terceros

En la Aerocivil se entiende por terceros las personas naturales o jurídicas con las que se establece un contrato, alianza o convenio. El objetivo de esta política es mantener la seguridad para los activos de información que sean compartidos o transferidos con estos terceros. Estas son las directrices:

4.24.1 Generales

- Aplicar el Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con Proveedores.
- Las políticas y procedimientos de seguridad de la información de la Aerocivil deben ser aplicadas por los terceros. Se debe incluir una cláusula contractual que exija el cumplimiento de estas políticas y es responsabilidad del supervisor del contrato que sea monitoreada esta condición.
- Se deben generar Acuerdos de Niveles de Servicio (ANS), Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con todos los terceros. Estos acuerdos deben contener una responsabilidad civil y penal para terceros y el monitoreo de su cumplimiento es responsabilidad del supervisor del contrato.
- Los riesgos de seguridad de la información relacionados con los terceros deben ser monitoreados constantemente durante la vigencia de la relación contractual. Este monitoreo es responsabilidad del supervisor del contrato, delegando las funciones correspondientes a los responsables de gestión de seguridad de la información, gestión de talento humano, gestión contractual y gestión de tecnologías de información.
- Los accesos requeridos por terceros a la información de la Entidad, sin importar su lugar de almacenamiento deben ser evaluados y aprobados de manera formal acorde a la Política de Control de Acceso de la Aerocivil.
- Los terceros deben cumplir con el uso aceptable de los activos de información que queden bajo su responsabilidad, esto define acciones como almacenamiento, transmisión, impresión y procesamiento.
- Incluir la gestión de vulnerabilidades de las plataformas que estén bajo su responsabilidad. Esto incluye el reporte oportuno a la Aerocivil de las vulnerabilidades identificadas y las medidas a implementar para mitigar los riesgos asociados, mientras se generan los parches o actualizaciones requeridos.
- El proveedor debe entregar a la Aerocivil la documentación de los procesos y procedimientos con los registros correspondientes, donde se demuestre el cumplimiento de las políticas de seguridad de la información en toda la cadena de suministro que involucre los servicios contratados.
- El proveedor debe entregar las herramientas para que la Aerocivil pueda hacer un seguimiento permanente de las actividades ejecutadas dentro del contrato y con la capacidad de verificar el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) para confidencialidad, integridad y disponibilidad de los activos de información involucrados en el contrato.
- Para la ejecución de controles de cambios se deben seguir las directrices de planeación estipuladas a nivel contractual y el Procedimiento de Gestión de Cambios de la Aerocivil.

- Reportar los eventos de seguridad de la información a la mesa de servicio de la Aerocivil, de acuerdo con el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

4.24.2 Continuidad en el servicio

Este numeral únicamente aplica para los terceros contratistas y proveedores.

- El tercero contará con un Plan de Continuidad de Negocio de acuerdo con el bien, servicio u obra adquirido por la Aerocivil.
- Cuando ocurra un evento de interrupción de los servicios prestados por el tercero que sea imputable totalmente a éste, asegurará la prestación del servicio cumpliendo con el Tiempo Objetivo de Recuperación (RTO) requerido por el (los) proceso (s) de la Aerocivil según las necesidades expuestas en el documento de Análisis de Impacto al Negocio – BIA.
- El tercero deberá informar los datos de contacto (teléfono, celular, mail y otros medios de contacto), así como horarios de disponibilidad de la(s) persona(s) responsable(s) que durante la vigencia del contrato atenderá(n) situaciones de crisis y/o de interrupción en los servicios suministrados, quien estará disponible durante las situaciones en mención y debe tener conocimientos técnicos específicos del servicio prestado a la Aerocivil.
- El tercero se obliga a entregar a la Aerocivil el resultado de las pruebas a su Plan de Continuidad de Negocio.
- Durante la vigencia del contrato, el tercero realizará al menos una prueba de continuidad de servicio, involucrando a los servidores públicos que la Aerocivil designe para ello, ya sea como observadores o participantes activos, siguiendo una metodología para la programación y planeación de pruebas.

4.24.3 Contratos.

- Se debe evitar el uso del adjetivo “seguro” como un parámetro de cumplimiento debido a que este no define ningún tipo de responsabilidad, se debe especificar con términos concretos y medibles a que se refiere esa condición de seguridad.
- Se deben especificar los mecanismos establecidos para proteger la confidencialidad y la integridad de la información en los sistemas de información.
- El proveedor debe establecer porcentualmente el nivel de disponibilidad comprometido para los servicios contratados.
- El proveedor debe establecer contractualmente el cumplimiento de los controles de seguridad de la información definidos.

4.25 Requerimientos funcionales del software

Es responsabilidad de quien requiere el Software (Sistema de Información, Aplicación local o en la nube y en general cualquier servicio informático como Internet, correo electrónico, herramientas colaborativas, mensajería instantánea y almacenamiento entre otros) o del Líder del Proceso que establece la necesidad para su uso, definir los requerimientos funcionales correspondientes. Los lineamientos para esta política son:

- Entregar a la Dirección de Informática los datos para definir la capacidad de almacenamiento, procesamiento y comunicaciones requeridos para el software; estos datos tendrán que ver con el número de usuarios, el tiempo de retención de los datos, el tipo y frecuencia de servicios utilizados, el tamaño de los archivos manejados y los tiempos de respuesta.
- Reportar a la Dirección de Informática los cambios que surjan sobre las condiciones establecidas inicialmente para la adquisición o desarrollo de software, de forma que haga la planeación de capacidad correspondiente y tome las medidas oportunas.
- La Dirección de Informática entregará reportes sobre el consumo de capacidades de almacenamiento para que el responsable del software verifique si las previsiones establecidas son las apropiadas o en caso contrario se tomen las medidas oportunas.
- Es responsabilidad de los Líderes de Proceso, solicitar con el mayor nivel de precisión posible los requerimientos del software para evitar gastos innecesarios o afectaciones de la operación por insuficiencia de recursos.

4.26 Responsabilidad de los colaboradores

Se hace uso del término colaborador para referirse a: Servidores Públicos, Contratistas y Estudiantes en Pasantía, se definen las siguientes directrices sobre su responsabilidad con la seguridad de la información en la Aerocivil:

- Cumplir estrictamente con los roles y responsabilidades de seguridad de la información que le correspondan al cargo o función asignado(a).
- Conocer, entender y aplicar el Marco Legal y Regulatorio de Seguridad de la Información aplicable a la Aerocivil.
- Conocer y aplicar la Metodología de Gestión de Activos de Información y la Guía de Gestión de Riesgos de Seguridad de la Información adoptados por la Aerocivil, para el o los procesos que estén bajo su responsabilidad.
- Tener pleno conocimiento y manejo del Inventario de Activos de Información y Matriz de Riesgos de Seguridad de la Información para el o los procesos que estén bajo su responsabilidad.
- Demostrar la debida diligencia frente a los riesgos e incidentes de seguridad de la información y hacer seguimiento y cumplir con lo que aplique para los planes de tratamiento de riesgos de seguridad de la información de acuerdo con su responsabilidad en los procesos.
- Desarrollar las habilidades y conocimientos necesarios para el manejo de herramientas de seguridad informática requeridas para el desempeño de sus funciones y mantenerse actualizado sobre su uso y el uso seguro de los recursos informáticos.
- Reportar y hacer seguimiento las anomalías que puedan comprometer la seguridad de la información de la Aerocivil.

4.27 Seguridad Física

Estos son los lineamientos que se deben cumplir en la Aerocivil para la seguridad física requerida para el procesamiento de información:

- Todos los colaboradores son responsables por la detección y reporte de anomalías sobre el acceso físico a las instalaciones y edificios de la Aerocivil.
- Los entornos físicos de procesamiento de información deben cumplir con las especificaciones en cuanto a temperatura, humedad relativa y protección física establecidas por los fabricantes.
- Se debe guardar un registro digital del acceso a los edificios y a las instalaciones de procesamiento de información de la Aerocivil.
- Todas las personas que ingresen a las instalaciones y edificios de la Aerocivil lo deben hacer cumpliendo con el Procedimiento de Control de Acceso Físico.
- Los colaboradores son responsables de la seguridad física de los equipos que le sean asignados cumpliendo con los procedimientos y estándares definidos en el MSPI.

4.28 Servicio de red para ciudadanos

Teniendo en cuenta los requerimientos legales para brindar servicios de acceso a red para los ciudadanos por parte de la Aerocivil, se establecen los siguientes lineamientos:

- Para el uso de este servicio es obligatorio el entendimiento y aplicación de la presente política.
- Este servicio debe cumplir con las Políticas de Seguridad de la Información de la Aerocivil.
- Los sitios donde funcione este servicio deben estar autorizados formalmente por la Aerocivil.
- La Aerocivil cumple con el tratamiento de los riesgos de seguridad de la información para este servicio, sin embargo, el usuario debe consentir que existen riesgos que deben ser aceptados.
- El usuario es responsable de la seguridad del dispositivo con el que haga uso de este servicio, se recomienda el uso de software debidamente licenciado y actualizado que incluya protección antimalware y el uso de controles criptográficos.
- El usuario se obliga al cumplimiento del Marco legal y Regulatorio Colombiano aplicable a seguridad de la información destacando entre otros: derechos de autor, ley de delitos informáticos y protección de datos personales.
- La Aerocivil no es responsable por la afectación que tenga un usuario ante el incumplimiento de esta política.

4.29 Servicios en la nube

La protección de la información bajo la responsabilidad de la Aerocivil debe garantizarse independiente del sitio donde se encuentre por tal motivo esta política busca garantizar que los datos creados, almacenados, actualizados, eliminados y procesados a través de servicios en la nube, cuente con los controles de protección para la integridad, confidencialidad y disponibilidad acorde con los lineamientos del MSPI.

- El contrato o licencia de alquiler en la nube, sin importar el tipo de plataforma, infraestructura o servicio, debe ser revisado y tener el visto bueno del Asesor Legal asignado.

- Verificar que el proveedor de los servicios en la nube cumple con la Política de Controles Criptográficos.
- Los servicios en la nube contratados deben cumplir con la Política de Control de Acceso para los activos de información que aplique.
- Si se almacena información clasificada en los niveles medio y alto frente a la confidencialidad esta debe mantenerse cifrada.
- Si la información va a ser accedida por dispositivos externos a la Entidad, se debe garantizar el cumplimiento de la Política de Dispositivos Móviles.
- Todos los servicios en la nube deben contar con el registro detallado de las acciones ejecutadas acorde con los requerimientos de seguridad de la información de los activos involucrados.
- Los servicios en la nube deben contar con los controles de verificación de la Integridad como hashing o firma digital para los activos de información que lo requieran.
- Los servicios en la nube deben contar con los controles para mantener los niveles de disponibilidad definidos por los procesos responsables de la información.
- La seguridad de los servicios en la nube debe mantener el esquema de seguridad perimetral acorde con los planes de tratamiento de riesgos para los activos de información involucrados, esto normalmente exige la implementación de servicios de FireWall de Red, FireWall de Aplicaciones, VPN, IDS/IPS, Antimalware, Correlación de Eventos y DLP.
- Los servicios en la nube deben tener la restricción del lugar geográfico de acuerdo con el perfil del usuario correspondiente.

4.30 Trabajo remoto

Los colaboradores autorizados para ejercer su trabajo por fuera de las instalaciones de la Aerocivil (esto incluye lo que está reglamentado en Colombia como Teletrabajo y Trabajo desde casa) deben hacerlo manteniendo los controles de seguridad de la información establecidos para los procesos dentro de los cuales desempeña sus labores. Las directrices son:

- El trabajo remoto para cualquiera de los colaboradores de la Entidad debe estar autorizado por el Director de Área o Jefe de Oficina y debe contar con el soporte de la Dirección de Informática y la Dirección de Talento Humano para colaboradores directos o la Dirección Administrativa para los demás colaboradores.
- Las conexiones para el trabajo remoto deben tener claramente identificadas el nombre y cargo del colaborador, las aplicaciones autorizadas, fechas de inicio y finalización, días y horarios autorizados para este esquema de trabajo.
- El jefe inmediato debe validar que los requerimientos solicitados están acordes a las funciones asignadas al rol correspondiente.
- El equipo utilizado para el trabajo remoto debe ser el asignado formalmente por la Aerocivil para hacer uso del software de escritorio virtual adoptado por la Entidad.
- No es permitido que la sesión establecida con la Aerocivil sea utilizada por una persona diferente al colaborador autorizado.

- El acceso remoto debe hacerse desde sitios autorizados dentro de los estándares definidos en el Sistema de Gestión de Seguridad de la Información.
- Reportar cualquier evento anormal aplicando la Política de Gestión de Incidentes de Seguridad de la Información.

4.31 Transferencia de Información

Para el cumplimiento de sus obligaciones la Aerocivil intercambia información con terceros y al interior de la Entidad, por diversos medios, esto debe hacerse aplicando los controles establecidos para la protección de la confidencialidad, integridad y disponibilidad de la información.

- Se debe seguir el Procedimiento para Transferencia de Información de la Aerocivil.
- El envío de la información clasificada o reservada debe hacerse haciendo uso de cifrado con un algoritmo criptográfico fuerte.
- El intercambio de información entre colaboradores de la Aerocivil y con terceros debe estar justificado por actividades formalmente establecidas en el desarrollo de las funciones y estar autorizado por el propietario de la información.
- Para el intercambio de información se debe aplicar lo establecido por el propietario de la información de acuerdo con las reglas de uso aceptable correspondientes que se definen dentro de la Política de Gestión de Activos.
- Se debe restringir el intercambio de información impresa considerando las vulnerabilidades que este medio trae.
- Todo el intercambio debe guardar una trazabilidad para auditorías, reportes a entes de control o una potencial gestión de incidentes de seguridad de la información.
- El intercambio de información clasificada con nivel alto de integridad debe estar protegido con firma digital.

4.32 Tratamiento de Datos Personales

La Aerocivil, entiende la importancia de definir los lineamientos necesarios para garantizar el cumplimiento a los requerimientos legales de la Ley 1581 del 2012 sobre protección de datos personales, por lo que se buscará siempre además del cumplimiento de las normas vigentes en esta materia, la adopción de buenas prácticas de seguridad de la información. A continuación, se presentan los principios de acuerdo con la Ley 1581 de 2012:

4.32.1 Legalidad

- La Aerocivil para el cumplimiento de esta política se basa en el Marco Legal y Regulatorio Colombiano aplicable a la protección de datos personales y establece una actualización permanente para cumplir con las disposiciones que el gobierno colombiano defina y apliquen en este ámbito.

4.32.2 Finalidad

- Los colaboradores solo deben usar información personal entregada por la Aerocivil para fines propios del cargo que desempeñen y las actividades, procesos y proyectos que se le hayan asignado formalmente.
- Dar lineamientos para la recolección de la información personal solo a través de las herramientas brindadas o avaladas por la Aerocivil.
- Solo se deben tratar los datos personales de acuerdo con las finalidades autorizadas por el titular o con fundamento legal.

4.32.3 Veracidad

- Esta propiedad es responsabilidad del Líder del Proceso cumpliendo con la debida diligencia para que se implementen los mecanismos y herramientas que garanticen la veracidad de los datos personales en todos los ámbitos y no solo en el de seguridad de la información. La seguridad de la información cumple con proteger la confidencialidad, integridad y disponibilidad de los datos personales, la veracidad de estos debe ser gestionada por cada proceso considerando este planteamiento.

4.32.4 Libertad

- Garantizar que los procesos, procedimientos y actividades de la Aerocivil, cumplan las directrices sobre protección de datos personales.
- Garantizar que los colaboradores se limiten a ejecutar los procesos, procedimientos y actividades definidos formalmente para el tratamiento de datos personales.
- Garantizar que los soportes de la autorización de tratamiento de datos personales sean debidamente almacenados y estén protegidos ante pérdida, daño o modificación y sean relacionados y tratados como un activo de información; se debe propender por el uso de medios digitales, considerando las vulnerabilidades de los documentos físicos.
- Implementar los canales de atención para informar a la ciudadanía sobre los datos personales tratados por la Aerocivil y cumplir con los requerimientos del titular acorde con la Ley 1581 de 2012.

4.32.5 Transparencia

- Capacitar a los colaboradores de las líneas de atención de la Aerocivil para que direccionen los requerimientos de protección de datos personales a las áreas designadas.
- Se deben implementar los mecanismos para brindar toda la información relacionada con datos personales tratados por la Aerocivil al titular correspondiente.

4.32.6 Acceso y Circulación Restringida

- Garantizar que la entrega o puesta en conocimiento de información personal a entes de inspección, vigilancia y control cuente con un deber legal o judicial de entrega de información.

- Garantizar que, ante la necesidad de entregar información personal a terceros, se cuente con un contrato de transmisión o transferencia de datos personales según sea la necesidad.
- Ante una solicitud de un ente de control, se deberá verificar si la información solicitada reposa en bases de datos estatales, de consulta pública o de información ya entregada anteriormente, a fin de redireccionar su petición a la consulta directa de dichos repositorios.
- Cualquier tercero que se enmarque en la figura de encargado del tratamiento de acuerdo con las definiciones indicadas en la Ley 1581 del 2012, deberá incluir dentro de su contrato, la transmisión de datos personales y demás responsabilidades relacionadas con el cumplimiento de la protección de estos datos.

4.32.7 Seguridad

Aunque todo lo que se establece en este documento es sobre seguridad de la información, se hace la referencia a este término de acuerdo con los principios que establece la Ley 1581 de 2012:

- Los datos personales pueden almacenarse en medios extraíbles solo si están cifrados.
- Los datos personales no pueden ser almacenados en equipos de usuario final, únicamente en servidores autorizados por el Líder del Proceso responsable de la custodia de estos datos.
- Los datos personales solamente pueden ser impresos si esta acción se encuentra establecida formalmente en el proceso responsable de la custodia de estos datos.
- Notificar a la mesa de servicio de la Dirección de Informática, cualquier intento de violación de seguridad de los datos personales (destrucción, pérdida, alteración, acceso o comunicación no autorizada).
- Mantener un inventario de datos personales por proceso, actividad, sistema de información, base de datos a su cargo, custodia o responsabilidad, en el cual se identifique el volumen, tipo de dato, responsable, encargado y finalidad del tratamiento.

4.32.8 Confidencialidad

Entendiendo que la confidencialidad es una de las propiedades de la seguridad de la información y que se encuentra inmersa en todos los planteamientos de esta política, se menciona este punto para alinearse con lo planteado en la Ley 1581 de 2012:

- Cada Líder de Proceso es responsable por definir las restricciones y privilegios de acceso sobre los datos personales que estén bajo su responsabilidad.
- Se debe restringir la impresión de datos personales y hacerlo si es indispensable considerando las vulnerabilidades que la documentación impresa conlleva para la confidencialidad.
- Se debe guardar un registro de todos los accesos sobre los datos personales.
- Cualquier tercero de la Aerocivil, que vaya a acceder o conocer información personal de tipo privado, semiprivado o sensible deberá contar con un acuerdo de confidencialidad.

4.33 Veracidad

La veracidad de la información es un atributo de calidad y es responsabilidad de todos los procesos velar por su cumplimiento; la seguridad contribuye con que se mantenga la confidencialidad, integridad y disponibilidad de la información, evitando que la veracidad sea afectada. Los procesos deben responsabilizarse por establecer los procedimientos, instrumentos, herramientas y mecanismos para garantizar la veracidad de los datos corporativos y personales, la seguridad de la información se encarga de preservarlos.

5. ASPECTOS IMPORTANTES

5.1 Excepciones

Si se presenta una situación que requiera una excepción que lleve al incumplimiento de una política de seguridad de la información, se deben documentar las condiciones sobre las cuales se presenta y especificar las circunstancias que justifican la decisión. Cada excepción conlleva un riesgo que debe tener un responsable, quien asume esta posición frente a la Dirección General y con la asesoría del Grupo Seguridad de la Información que presentará el panorama de la situación.

5.2 Incumplimiento

El incumplimiento de las políticas de seguridad de la información se considera una falta grave dentro de la Entidad y podrá incurrir en investigaciones de carácter disciplinario y legal en caso de que se requiera.

5.3 Responsabilidad

- **Comité Institucional de Gestión y Desempeño:** Responsable de la aprobación de las políticas de seguridad de la información. Debe definir el responsable para la ejecución de las auditorias de seguridad de la Información y el seguimiento al cumplimiento de los compromisos asignados en la matriz de riesgos de seguridad de la información.
- **Dirección de Informática y Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea:** Responsables de la implementación de controles tecnológicos de los activos de información.
- **Dirección Administrativa y Dirección de Servicios Aeroportuarios:** Responsables de la seguridad física, cámaras de vigilancia y controles de acceso físico.
- **Dirección de Talento Humano:** Responsable de la capacitación y sensibilización en los temas relacionados con seguridad de la información.
- **Grupo Seguridad de la Información:** Responsable de gestión de incidentes de seguridad, seguimiento a la implementación de controles de seguridad, apoyo a las áreas en el cumplimiento de las obligaciones relacionadas con seguridad de la información y actualización de las políticas de seguridad de la información.