Contenido

1. OBJETIVO

Establecer las políticas y lineamientos de seguridad de la información en la Corporación de la Industria Aeronáutica Colombiana, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información dando cumplimiento al Modelo de Seguridad y Privacidad de la Información – MSPI de Gobierno Digital

2. DOCUMENTOS DE REFERENCIA

Gobierno Digital

Modelo de Seguridad y Privacidad de la Información – MSPI

Estándar Internacional de Seguridad BASC 5.0.1

Norma ISO IEC 27001:2013

3. JUSTIFICACIÓN

La Corporación de la Industria Aeronáutica Colombiana - CIAC S.A., reconoce la información como un componente indispensable de la gestión conducente al logro de los objetivos institucionales, razón por la cual es necesario establecer lineamientos que aseguren la protección de la información de manera adecuada, independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada, garantizando la confidencialidad, integridad, disponibilidad y privacidad de esta.

4. ALCANCE

Este manual contempla las políticas y directrices para la seguridad de la información en la CIAC, cubriendo los aspectos administrativos y de control que deben ser cumplidos por los funcionarios, colaboradores, pasantes y demás partes interesadas que tengan relación con la Corporación.

5. DEFINICIONES

Activo de Información: Es todo aquello que tiene valor para la Corporación y que, por lo tanto, requiere de protección.

Autenticidad: Es la garantía que el mensaje ha sido enviado por quien dice ser.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a personas, entidades o procesos autorizados. (ISO/IEC 27000)

Copia de Seguridad (Backup): Duplicado de los datos que se hace para poder recuperarlos ante cualquier pérdida o incidente.[1]

Custodio: Es la unidad organizacional o proceso, designado por la Corporación para mantener las medidas de protección necesarias sobre los activos de información confiados.

Ciberseguridad: conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la Corporación en el Ciberespacio[2]

Directriz: Instrucción o norma que ha de seguirse en la ejecución de algo[3]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera (ISO/IEC 27000)

Dispositivo Móvil: Dispositivo destinado a almacenar y reproducir archivos digitales como audio, imágenes y vídeo, con la capacidad de conectarse a internet, permitiendo enviar y compartir los archivos capturados. Los dispositivos móviles más utilizados son los computadores portátiles, tabletas, cámaras, teléfonos inteligentes o smartphones, reproductores inteligentes, entre otros.

Firewall: Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno[4]

[1] Tomado de www.ticportal.es/glosario-tic/copia-seguridad-backup
[2] Tomado de Glosario (mintic.gov.co)
[3] RAE
[4] Tomado de Glosario (mintic.gov.co)

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27000)

OJT: On the Job Training SAP, Entrenamiento para desempeño según funciones de usuario.

OneDrive: Herramienta de almacenamiento en la nube y uso compartido de archivos

Malware: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.[5]

Página Web: Conjunto de informaciones de un sitio web que se muestran en una pantalla y que puede incluir textos, contenidos audiovisuales y enlaces con otras páginas.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Propietario: Es una parte designada de la Corporación, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Recursos Tecnológicos: Componentes de hardware y software tales como servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros; los cuales tienen como finalidad apoyar las tareas

[5] Tomado de Glosario (mintic.gov.co)

administrativas y logísticas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Corporación.

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000)

Seguridad Digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Sistema de información. Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información requiriendo a su vez de la interacción de uno o más activos de información para efectuar las tareas previstas. Puede ser de origen interno o de origen externo conforme a las necesidades de la Corporación.

Sitio Web: Conjunto de páginas web agrupadas bajo un mismo dominio de internet[6]

6. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

La Corporación de la Industria Aeronáutica Colombiana entendiendo la importancia de una adecuada gestión de la información, se ha comprometido en la implementación del Modelo de la Seguridad y Privacidad de la Información – MSPI para la protección de los activos de información que soportan los procesos de la Corporación, mediante la gestión de riesgos e incidentes y el fortalecimiento de la cultura de seguridad de la información en los funcionarios, colaboradores, contratistas, pasantes, clientes, y demás partes interesadas para mantener la integridad, confidencialidad, disponibilidad y privacidad de los datos con políticas, procedimientos y directrices referentes a la seguridad de la información que permiten el mejoramiento continuo y el cumplimiento de los objetivos misionales.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

La CIAC, mediante la Gestión de Talento Humano establece las acciones para asegurar que los funcionarios, colaboradores, contratistas y pasantes comprendan sus responsabilidades de seguridad de la información y sean idóneos en los roles

[6] RAE

asignados, mediante los procedimientos de selección, vinculación e inducción de personal.

Gestión de Talento Humano debe reportar todas las novedades de ingreso y retiro de personal de manera inmediata a la Gestión TIC's, con el fin de gestionar las acciones relacionadas con la seguridad de la información.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La CIAC identifica los activos de información, con el fin de clasificarlos y protegerlos, de acuerdo con su importancia para evitar la divulgación, modificación, retiro o destrucción no autorizada de la información, estableciendo criterios y directrices para el tratamiento de estos.

8.1 Responsabilidad de Activos de Información

- La información que se genere procese, almacene, transfiera o transmita en medios físicos o digitales, o por su plataforma tecnológica es de propiedad de la CIAC y solo puede ser utilizada para el cumplimiento de los objetivos corporativos.
- Los coordinadores, jefes o directores de área, oficina o grupo actúan como propietarios de los activos de información, por lo tanto, deben llevar a cabo el control y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas con el apoyo de su personal.
- Todos los sistemas de información necesariamente deben tener asignado un "responsable", el cual es el encargado de definir los niveles de privacidad de la información, así como los usuarios y permisos que cada uno deba tener.
- Los jefes y coordinadores de oficina deben recibir los recursos tecnológicos asignados a sus colaboradores por activos fijos cuando estos se retiran de la Corporación o son trasladados de área.
- Gestión TIC's resguarda los activos de información correspondientes a la plataforma tecnológica de la Corporación, con el fin de asegurar su apropiada operación y administración.
- Gestión TIC's establece una configuración adecuada para los recursos tecnológicos con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- Gestión TIC's realiza revisiones periódicas con el fin de verificar el cumplimiento de las políticas y directrices de seguridad y privacidad de la información.
- Los funcionarios, colaboradores, contratistas y pasantes deben hacer uso adecuado y eficiente de los recursos tecnológicos asignados para el desarrollo de las actividades asignadas.
- Los funcionarios, colaboradores, contratistas y pasantes no podrán instalar ningún programa o software, en los recursos tecnológicos sin la aprobación de Gestión TIC's.
- El usuario debe reportar de forma inmediata al Grupo de Gestión Administrativa y al Grupo de Gestión TIC´s, según sea el caso, cuando se detecte riesgo real o potencial sobre equipos de cómputo, de comunicaciones o algún tipo de recurso tecnológico, tales como caídas de agua, choques eléctricos, golpes, robos de partes, peligro de incendio o cualquier tipo de evento que se prevea puede ocasionar daño a cualquier recurso tecnológico de la Corporación.
- Todos los usuarios deben reportar a la Gestión TIC's cualquier evento que pueda afectar la confidencialidad, integridad y disponibilidad de cualquier tipo de activo de información.
- Los usuarios no pueden subir ningún tipo de información de la Corporación en cualquier sitio de la nube que no sea de acceso Institucional o para el cumplimiento de las labores autorizadas por la CIAC.
- Los dispositivos como computadores, teléfonos inteligentes o smartphones y tabletas, donde se configure la cuenta de OFFICE 365 corporativa serán monitoreados para evitar posibles fugas de información. En caso de encontrarse anomalías en el uso de las herramientas, la cuenta de OFFICE 365 se desvinculará del dispositivo.
- El usuario es responsable de no enviar información clasificada, reservada o sensible por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
- Los funcionarios, colaboradores, contratistas y pasantes deben devolver todos los activos de información (información, activos fijos, entre otros) que se encuentren a su cargo al momento de terminar su vinculación con la Corporación o son trasladados de área.

8.2 Uso de Dispositivos Móviles

Se establecen las siguientes directrices para el uso de dispositivos móviles como computadores portátiles, tabletas, teléfonos inteligentes o smartphones:

- Los usuarios no pueden realizar ningún cambio o alteración física de los componentes de los dispositivos móviles corporativos.
- La APP para acceder al correo electrónico corporativo desde el teléfono inteligente o smartphone no puede tener alteraciones en el código.
- Los dispositivos móviles no pueden dejarse expuestos a la utilización por parte de terceros con el fin de preservar la seguridad digital de la información.
- Los usuarios deben evitar usar los dispositivos móviles corporativos en lugares que no ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- El usuario no puede modificar las configuraciones de seguridad de los dispositivos móviles corporativos que estén bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega, además de no instalar software que no tenga el debido licenciamiento.
- El usuario debe utilizar los dispositivos corporativos solamente para las funciones asignadas o el cumplimiento de los objetivos corporativos.
- Gestión TIC’s instala un programa de antivirus en los dispositivos móviles corporativos teniendo en cuenta las características de cada dispositivo.
- Gestión TIC’s dispone para los usuario de Android y IOS el antivirus Kaspersky para protección del dispositivo, en caso de utilizar las herramientas corporativas en los dispositivos móviles personales.

8.3 Uso de Recursos Informáticos

Se establecen las siguientes directrices para el uso adecuado de los recursos informáticos:

- Gestión TIC’s es el único grupo autorizado para instalar, configurar y dar mantenimiento a los recursos informáticos de la Corporación.
- El usuario no debe realizar ninguna alteración física de los componentes de los equipos de cómputo.

- Solo se instala software autorizado y licenciado para uso institucional siempre y cuando cumpla con todos los requisitos de legalidad.
- Descargar o instalar archivos ajenos a las labores institucionales como fotos, videos, música o programas (incluyendo los de descarga masiva o material de entretenimiento)
- No está permitido instalar programas maliciosos como virus informáticos, gusanos, phishing, keyloggers o cualquier tipo de malware en los servicios tecnológicos.

8.4 Uso del Correo Electrónico Corporativo

La Corporación, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre colaboradores y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico siendo el autorizado el correo corporativo bajo el dominio @ciac.gov.co, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Se deben seguir las siguientes directrices para el uso del correo electrónico corporativo:

- Para la creación de cuentas de correo electrónico, se requiere que un funcionario o colaborador del área, oficina o grupo realicen la solicitud mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), adjuntando el acta de asignación del equipo de cómputo emitida por Activos Fijos.
- Las cuentas se crean de acuerdo con la disponibilidad de licenciamiento del correo. El nombre de la cuenta se genera con el cargo o las funciones a desempeñar por ejemplo cargo@ciac.gov.co o función@ciac.gov.co, no es personalizada con los datos del personal como nombre.apellido@ciac.gov.co.
- La cuenta de correo electrónico corporativo asignada es de carácter individual. Por consiguiente, ningún funcionario, colaborador, contratista o provisto por un tercero, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya, ni el correo personal para asuntos de la

Corporación o de las funciones para el desempeño de sus labores u obligaciones.

- Los mensajes y la información contenida en el buzón del correo electrónico corporativo solamente deben estar relacionados con el desarrollo de las funciones en apoyo al objetivo misional de la Corporación, por lo tanto, no debe ser utilizado para actividades personales.
- Está prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas.
- La cuenta de correo electrónico corporativo asignada es de carácter individual, y el usuario al que se le asigna es el responsable de su administración y no debe permitir que otro usuario envíe correos utilizando su cuenta.
- Está prohibido intentar acceder o acceder sin autorización a otra cuenta de correo electrónico diferente a la asignada.
- No está permitido enviar mensajes de correo con información sensible o confidencial sin la autorización expresa del propietario de la información.
- Solamente está autorizado el uso de correos corporativos, en cuanto a los correos con dirección de Gmail, Hotmail, Yahoo, entre otros, están sujetos a la verificación del contenido, tanto para envío o recepción por Gestión TIC's para su aprobación o rechazo.
- Se restringe el uso de correos electrónicos diferentes al correo corporativo como Gmail, Hotmail, Yahoo, entre otros, tanto para enviar como para recibir mensajes, lo cual se gestiona mediante una regla definida en el Firewall del correo. Se exceptúan los correos autorizados por Gestión TIC's, los cuales se colocan como listas blancas en el Firewall del correo como clientes o aliados estratégicos para el core del negocio.

8.5 Uso Adecuado de Internet

La Corporación consciente de la importancia de la Internet como una de las herramientas clave para su desempeño proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en sus puestos de trabajo

Se establecen las siguientes directrices para el uso adecuado de Internet:

- El internet debe utilizarse únicamente para las labores asignadas y cumplimiento de los objetivos institucionales.
- Los perfiles de navegación se ajustan dependiendo del cargo que ocupe el usuario.
- En caso de requerirse el acceso a un sitio web específico se debe realizar la solicitud mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), justificando la necesidad para la verificación, aprobación y habilitación por parte de Gestión TIC's.
- No está permitida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o software que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- CIAC mediante Gestión TIC's supervisa el uso y acceso del servicio de internet para verificar que el servicio está siendo usado apropiadamente para el cumplimiento de las funciones y objetivos corporativos, respetando siempre los derechos a la intimidad y a la privacidad.
- No se permite el acceso a sitios o páginas web relacionadas con pornografía, drogas, alcohol, webproxys, hacking, grupos extremistas y/o cualquier otra página que vaya en contra de la ética, moral, las leyes vigentes, normas, políticas o directrices establecidas.
- La herramienta de mensajería instantánea autorizada es Microsoft Teams, que permite la comunicación y la colaboración en tiempo real entre usuarios dentro y fuera de la Corporación.
- Está restringido el acceso y el uso de redes sociales o mensajería instantánea tales como Facebook, Instagram, Twitter, Skype, Telegram, LINE y otros similares, que tengan como objetivo la comunicación entre personas y el intercambio de información. Solo está permito el acceso a la Coordinación de Comunicaciones para el manejo de las redes sociales corporativas relacionadas con las actividades propias del core de la Corporación.

8.6 Clasificación y Manejo de la Información

Teniendo en cuenta que la información es uno de los activos más importante de una organización y que hace parte fundamental de la operación, el Grupo Asesor Jurídico mediante el instructivo I-1-07-001 Clasificación de la Información, establece las políticas para la gestión segura de la información propiedad de la Corporación de la Industria Aeronáutica Colombiana, cualquiera que sea su forma en la que se encuentre contenida.

8.7 Medios de Almacenamiento

La CIAC, establece directrices para evitar la divulgación, modificación, retiro o destrucción no autorizados de información almacenada en los diferentes medios.

8.7.1 Medios de Almacenamiento Removibles

- Los medios de almacenamiento removibles como USB, SD, microSD, discos duros removibles, CDs y DVDs, están restringidos y los puertos donde se conectan estos medios en los equipos de cómputo se encuentran bloqueados, debido a que pueden ser utilizados para extraer información no autorizada y generar incidentes de seguridad.
- En caso de necesitarse la habilitación de estos puertos para necesidades especiales que se requieran para el cumplimiento de los objetivos misionales de la Corporación, el usuario debe realizar la solicitud mediante oficio a la Gerencia o Subgerencia con el VoBo del Coordinador de Gestión TIC’s, para la autorización del respectivo desbloqueo.
- Para la transferencia de información de un dispositivo extraíble se debe gestionar por medio de Gestión TIC’s, quienes llevan el registro y control, y copiarán los datos en una carpeta de red.

8.7.2 Medio de Almacenamiento en la Nube

CIAC proporciona como medio de almacenamiento en la nube, la herramienta OneDrive para usuarios de OFFICE 365 que permite acceder y compartir los archivos de una forma segura y en tiempo real.

Se prohíbe el uso de cualquier medio de almacenamiento en la nube que no esté debidamente controlada y autorizada por la Gestión TIC's para el manejo de la información de la Corporación.

8.7.3 Unidad de Almacenamiento Conectado en Red

CIAC cuenta con la QNAP como unidad de almacenamiento conectado a red, donde se almacenan las copias de seguridad como uno de los medios de respaldo de la información con los que cuenta la Corporación.

9. CONTROL DE ACCESO

La CIAC asegurará y limitará mediante privilegios el acceso a las redes de datos, recursos tecnológicos y sistemas de información, velando porque los usuarios tengan solamente el acceso autorizado.

9.1 Perfiles para el Acceso a Usuarios

Es responsabilidad del coordinador, jefe o director de área, oficina o grupo gestionar los permisos para cada usuario mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), como control de autorización de los perfiles. Los perfiles se asignan teniendo en cuenta la naturaleza del cargo, las funciones u obligaciones contractuales para el cumplimiento de los objetivos misionales de la Corporación.

Para la gestión de acceso a los usuarios se establecen los siguientes perfiles básicos:

Administrador TIC's: Perfil con privilegios elevados para instalación de software, gestión y monitoreo de servidores, aplicaciones, redes, equipos de cómputo, impresoras y sistemas operativos.

Administrador ISolución: Perfil para gestionar la información del Sistema Gestión de la Calidad, con privilegios para crear, modificar y asignar permisos en el sistema a cada uno de los usuarios acorde a las funciones u obligaciones contractuales para el cumplimiento de los objetivos misionales de la Corporación.

Administrador ORFEO: Perfil para la gestión documental, con privilegios para crear, modificar y asignar permisos en el sistema a cada uno de los usuarios acorde

a las funciones u obligaciones contractuales para el cumplimiento de los objetivos misionales de la Corporación.

Administrador SAP: Gestionar la seguridad del ERP SAP, mediante el monitoreo, creación, actualización, modificación de los roles y perfiles de autorización, al igual que asignar las transacciones según los procesos que realiza cada uno de los usuarios dentro de la Corporación.

Directivos: Perfil con menores limitaciones en la navegación en internet acorde al cumplimiento objetivos misionales de la Corporación, con la facultad para gestionar las autorizaciones de sus colaboradores. De igual manera, se asigna acceso al correo electrónico corporativo y a la intranet, con restricción para instalar cualquier tipo de software en los equipos de cómputo.

Colaboradores: Perfil con limitaciones para la navegación en internet acorde al cumplimiento objetivos misionales de la Corporación. Adicionalmente, se asigna acceso al correo electrónico corporativo y a la intranet, con restricción para instalar cualquier tipo de software en los equipos de cómputo.

9.2 Acceso a Redes y Servicios de Red

Se establecen las siguientes directrices para el acceso a las redes y servicios de red:

- CIAC dispondrá de los recursos necesarios para la correcta operación de la infraestructura tecnológica de red.
- Los equipos de cómputo que se conecten a las redes de datos deben estar dentro del dominio CIAC, estar protegidos por un antivirus y tener las últimas actualizaciones y parches de seguridad del sistema operativo y software.
- Gestión TIC’s es responsable de la activación y gestión de los puntos de red, los cuales están protegidos a través de la MAC del equipo de cómputo.
- Gestión TIC’s debe asegurar que las redes inalámbricas cuenten con métodos de autenticación para evitar el acceso no autorizado y/o utilización de dispositivos personales.
- Cuando se requiere hacer reubicación física de equipos de cómputo, debe realizarse la solicitud mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), para la configuración de los puertos y accesos a la red.

- Para los equipos de escritorio de propiedad de la Corporación está deshabilitada la conexión vía WIFI, salvo casos especiales en que los equipos no puedan conectarse por cable debido a limitaciones de la infraestructura física.

9.3 Gestión de Acceso a Usuarios

- Un funcionario o colaborador de área, oficina o grupo deben solicitar mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), la creación, modificación, activación o cancelación para el acceso a los recursos tecnológicos del personal nuevo o retirado.
- Para el caso de solicitudes del ERP SAP el Ticket debe ser autorizado por el líder funcional de la dependencia, teniendo en cuenta el documento POL-1-01-013 Administración de Licencias y Usuarios SAP (ERP, SUCESSFACTORS Y PAYROLL) en Isolución.
- Gestión TIC's suministrará los datos de acceso para el equipo de cómputo, intranet y correo electrónico.
- Para la asignación de accesos a los recursos tecnológicos, se aplicará el principio de mínimo privilegio necesario para la realización de las funciones o el cumplimiento de los objetivos misionales de la Corporación.
- Es responsabilidad del usuario hacer buen uso de los datos de acceso que se le asignan para el manejo de los recursos tecnológicos.
- Las contraseñas deben contener mínimo 9 caracteres, tener letras, números y caracteres especiales, y debe cambiarse cada 45 días.
- Gestión de Talento Humano informa a Gestión TIC's mediante la plataforma SuccessFactors, cuando el personal de planta y/o militar salen a período de vacaciones, licencias no remuneradas, incapacidades o cualquier otra novedad que implique suspender los accesos a los recursos Tecnológicos durante el período establecido.
- El coordinador, jefe o director de área, oficina o grupo debe informar mediante Ticket en la Mesa de Ayuda (Helpdesk TICS), licencias no remuneradas, incapacidades o cualquier otra novedad que implique suspender los accesos a los recursos Tecnológicos al personal contratado mediante compañías de outsourcing y personal por prestación de servicios.

- Para solicitudes de acceso para el ERP SAP, el Ticket debe contener el Formato OJT con la firma del líder funcional para la asignación de usuarios nuevos, indicando los roles de las transacciones según el cargo a desempeñar, los datos de identificación, teléfono de contacto, correo electrónico, nombre del cargo y dependencia.

10. CRIPTOGRAFIA

La CIAC vela porque la información clasificada como reservada o restringida, sea cifrada cuando esta salga de la Corporación, para proteger la confidencialidad, autenticidad y/o integridad de la información.

10.1 Uso de Token de Seguridad por USB

La Corporación provee las condiciones de manejo de los token de seguridad por USB para los procesos que los utilizan y vela para que se haga uso responsable de los mismos.

Se establecen las siguientes recomendaciones para el uso de los Token de Seguridad por USB:

- El responsable del uso del token de seguridad es el coordinador, director o jefe del área encargado del proceso y es el encargado de velar por la integridad del dispositivo.
- El usuario responsable del token, debe informar a Gestión TIC's mediante Ticket en la Mesa de Ayuda (Helpdesk TICS) para habilitar este dispositivo en el equipo designado.
- El usuario debe almacenar el token en lugar seguro fuera del alcance de terceros no autorizados.
- El token no debe ser usado fuera de las instalaciones de la CIA para evitar su pérdida o robo.
- En caso de pérdida o robo de estos dispositivos se debe informar a las entidades emisoras, con el fin de efectuar el respectivo bloqueo y reposición de estos.
- No se debe permitir que terceras personas vean la contraseña del token y aceptar ayuda de personas no autorizadas para la utilización de este.

- Es usuario es responsable de las transacciones electrónicas que se efectúen con el token asignado, por lo tanto, cualquier evento irregular con el uso de estos, será el usuario quién asumirá la responsabilidad administrativa, disciplinaria y económica que tal situación genere.
- El token debe mantenerse en un lugar seco, y no introducirlos en agua u otros líquidos, evitar exponerlos a campos magnéticos y a temperaturas extremas, además de evitar que sean golpeados o sometidos a esfuerzo físico.
- Cuando el token presente mal funcionamiento, caducidad, y/o cambio del titular o funciones, el coordinador, director o jefe del área encargado del proceso será el encargado de reportar a la entidad emisora para el cambio o devolución del dispositivo asignado.

10.2 Controles Criptográficos

- Cuando un computador portátil o una Tablet contenga información clasificada como reservada o restringida y sea retirado de la Corporación, esta información debe cifrarse.
- Gestión TIC's asesorará a los usuarios cuando requieran transmitir o enviar información reservada o restringida por vía electrónica para la aplicación de algún control criptográfico que se tenga como herramienta.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

La CIAC evitará el acceso físico no autorizado, la pérdida, daño, robo o exposición de los activos de información y la interrupción de las operaciones de la Corporación, al igual que controlará las amenazas externas y condiciones medioambientales que pongan en riesgo la infraestructura tecnológica y afecten la información.

11.1 Áreas Seguras

Se establecen las siguientes directrices para las áreas seguras:

- El acceso físico al Data Center principal y sus alternos, o a los Centros de Cableado deben ser aprobadas por Gestión TIC's.
- El ingreso al Data Center o a los Centros de Cableado para proveedores y visitantes es restringido, por lo que siempre deben estar acompañados por el

personal de Gestión TIC's, y hacer el registro en el libro destinado para el control de acceso.

- Las luces deben permanecer apagadas mientras no se encuentre personal dentro del Data Center.
- Se seguirán los lineamientos para el control de acceso y seguridad física establecidos en el M-1-03-007 Manual del Sistema de Gestión de Control y Seguridad y los establecidos por Seguridad Aeroportuaria e Instalaciones del Grupo de Gestión Administrativa y Financiera.

11.2 Seguridad de los Equipos

Se establecen las siguientes directrices para la seguridad de los equipos:

- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas que garanticen su integridad física.
- Los equipos portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exposición a fuertes campos magnéticos, líquidos, y prevenir la pérdida y/o hurto de estos
- Los usuarios deben informar de forma inmediata a Gestión TIC's en caso de detectarse riesgo real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas, golpes o peligro de incendio.
- Para retirar cualquier recurso tecnológico de las instalaciones de la CIAC, se debe diligenciar el F-2-04-067
- Los usuarios no deben intervenir las redes de cableado, instalar cables, cortar o empalmar cables, desprender marcaciones de tomas, así como cualquier otra acción que atente contra la integridad de las redes informáticas.

12. SEGURIDAD DE LAS OPERACIONES

12.1 Protección Frente a Ciberataques

La CIAC proporciona los mecanismos necesarios para garantizar la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y

almacena, mediante la adopción de controles que eviten la divulgación, modificación o daño permanente ocasionados por algún tipo de ciberataque utilizando diferentes métodos de códigos maliciosos. Así mismo, se genera una cultura de seguridad entre los usuarios frente a estos ataques.

Se establecen las siguientes directrices para la protección frente a ciberataques:

- Provee herramientas como antivirus, antimalware, antispam, antispyware, entre otras, que reducen el riesgo de contagio de software malicioso y respaldan la seguridad de la información.
- Verifica que los sistemas operativos y software, especialmente el del antivirus, antimalware, antispam, antispyware, entre otras, poseen las últimas actualizaciones y parches de seguridad.
- El usuario debe asegurarse que los archivos adjuntos de los correos electrónicos, descargados de sitios web o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos
- Gestión TIC's programa conferencias y campañas de sensibilización sobre temas de ciberseguridad, con el fin de generar conciencia entre los usuarios sobre el uso responsable del internet y los riegos a los que pueden estar expuestos.
- Notificar a Gestión TIC´s la sospecha o detección de alguna infección por software, correo malicioso o de dudosa procedencia, a fin de que se tomen las medidas de control correspondientes para cualquier ciberataque que se pueda presentar.

12.2 Copias de Seguridad (Backup) y Recuperación

La CIAC proporcionará los recursos necesarios y medios adecuados para generar copias de seguridad de la información crítica de la Corporación, asegurando que se puedan restaurar en caso de una falla y/o desastre, velando por la integridad, confidencialidad y disponibilidad de la información.

12.2.1 Copias de Seguridad (Backup)

Para realizar las copias de seguridad se deben seguir las siguientes directrices

- La CIAC proporciona como herramienta para llevar a cabo el proceso de copia de seguridad de la información OneDrive Corporativo con 1TB de almacenamiento en la nube para los usuarios que tienen asignada cuenta de OFFICE 365. Para los usuarios especiales que no cuentan con OFFICE 365 se dispone de un almacenamiento de 20 Gb en la ubicación \\SRV-20162\Users\UsuarioDeDominio.
- Gestión TIC's realiza campañas de sensibilización a los usuarios sobre la importancia de realizar las copias de seguridad.
- Cada usuario es responsable de hacer mínimo una vez cada trimestre las copias de seguridad o las que considere necesarias para mitigar el riesgo de pérdida de información.
- Gestión TIC's no se hace responsable por la información que no tenga el respectivo respaldo en OneDrive o en la herramienta proporcionada para las copias de seguridad.
- La copia de seguridad debe estar actualizada y relacionada únicamente con la información relevante para el cumplimiento de los objetivos de la Corporación, no debe contener información de índole personal, música, vídeos y fotos.
- El usuario puede realizar una copia local del correo electrónico utilizando el instructivo I-7-00-004 ubicado en ISolución.
- Gestión TIC's realiza copia incremental diaria de los servidores locales y virtuales, en las horas programadas con la herramienta Veem Backup o la herramienta disponible para tal fin. Esta herramienta se configura para que envíe correos de notificación al Grupo de Gestión TIC's con el informe de ejecución de la copia de seguridad, la cual se debe verificar todos los días.

Nombre Servidor Virtual	Tipo Backup	Hora Programa
VR-Orfeo	Hyper-V Backup	10:30 PM
VM-SRVAD365	Hyper-V Backup	10:00 PM

VM-SRVDC04	Hyper-V Backup	1:00 AM
VM-SRVDLPCIAC	Hyper-V Backup	10:10 PM
VM-SRVFSFD	Hyper-V Backup	1:00 AM
VM-SRVIMPAUR	Hyper-V Backup	1:01 AM
VM-SRVISODB	Hyper-V Backup	10:10 PM
VM-SRVME1	Hyper-V Backup	10:10 PM
VM-SRVME2	Hyper-V Backup	10:30 PM
VM-SRVTE	Hyper-V Backup	1:01 PM

- El proveedor de backup debe enviar los viernes de cada semana el informe de la copia de seguridad de la herramienta HERMES y el respaldo en la nube hacia ZEUS de todos los servidores y el repositorio que se encuentran en la QNAP.
- La copia de seguridad del ERP SAP es realizada por la empresa prestadora del servicio de Hosting de SAP, entregando una copia en medio físico de almacenamiento con el backup de tipo full o completo mes vencido. Así mismo, se cuenta con un servidor de respaldo asignado a la Corporación con una réplica de la información de producción ERP SAP en caso de alguna novedad o anomalía para que el servicio esté disponible.
- Las copias de respaldo a la Base de Datos y Logs de los servidores del ERP SAP se programan de lunes a domingo como se indica en la siguiente

imagen:

Ambiente	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Productivo	Database	Database	Database	Database	Database	Database	Database
	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)
Desarrollo		Database		Database			
	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)
Calidad					Database		
	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)
Solman	Database	Database	Database	Database	Database	Database	Database
	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)	Logs (3)

12.2.2 Restauración

- Para el ERP SAP la empresa prestadora del servicio de Hosting de SAP, es la encargada de realizar el proceso de restauración en caso de falla y/o desastre, garantizando la estabilidad del sistema.
- Gestión TIC's destinará un servidor virtual para realizar pruebas de restauración para verificar que las copias de seguridad estén ejecutándose correctamente y en caso de alguna eventualidad poder restablecer el servidor a un estado anterior. Estas pruebas se realizarán trimestralmente dejando el registro del nombre de servidor restaurado, la fecha de la copia recuperada y el informe del paso a paso de la restauración.

12.3 Gestión de Vulnerabilidad Técnica

La CIAC revisa las vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas de vulnerabilidad, con el fin de evaluar la exposición de la Corporación a estas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

Se establecen las siguientes directrices para la gestión de vulnerabilidades:

- Gestión TIC's realiza revisión mensual junto con el proveedor de seguridad perimetral y antivirus, donde se genera un informe mostrando el estado actual de la plataforma y los dispositivos tecnológicos para ejecutar acciones de mejora y cerrar las posibles brechas de seguridad.
- Gestión TIC's realiza pruebas semestrales de vulnerabilidades.

- Gestión TIC's toma medidas adecuadas para reducir los riesgos resultantes de las pruebas de vulnerabilidad.

13. SEGURIDAD DE LAS COMUNICACIONES

La CIAC propende por el aseguramiento y disponibilidad de las redes de datos y el control del tráfico, mediante mecanismos de seguridad que protegen la integridad y confidencialidad de la información que se transporta a través de estas redes, además establece acuerdos para el intercambio seguro de información dentro de la Corporación y con cualquier entidad externa.

13.1 Gestión en la Seguridad de Redes

Se establecen las siguientes directrices para la gestión seguridad de las comunicaciones:

- Mantener segmentada la red como control de seguridad.
- Implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos
- Identificar mecanismos de seguridad y niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Corporación, acogiendo buenas prácticas de configuración segura.
- Instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Corporación.
- Inhabilitar servicios, puertos y protocolos en las redes de datos que pongan en riesgo la seguridad y privacidad de la información.

13.2 Transferencia y/o Intercambio de Información

La CIAC implanta procedimientos y controles de seguridad que protegen la transferencia y/o intercambio de información mediante el uso de todo tipo de recursos de comunicación, además de establecer acuerdos de confidencialidad y acuerdos para la transferencia y/o intercambio seguro de información entre la Corporación y terceros.

Se establecen las siguientes directrices para la transferencia y/o intercambio de información:

- Los acuerdos de confidencialidad y acuerdo de transferencia y/o intercambio de información entre la CIAC terceros, deben incluir la prohibición de divulgación de la información entregada por la Corporación, además de las obligaciones, compromisos y responsabilidades civiles y penales por el incumplimiento de estos acuerdos.
- Utilizar medios de comunicación confiables y adoptar los controles necesarios para la protección de la confidencialidad e integridad de la información.
- Asegurar que los datos sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o por solicitud de entes de control.
- Verificar que se destruya la información de manera segura una vez esta cumpla con la función para la cual fue enviada.
- No debe utilizarse el correo electrónico o mensajería instantánea para enviar o recibir información sensible o confidencial de la Corporación o partes interesadas, sin los debidos controles de seguridad.

14. CUMPLIMIENTO

14.1 Cumplimiento de Requisitos Legales y Contractuales

La CIAC velará por la identificación, documentación y cumplimiento de la legislación aplicable y requisitos contractuales referentes a los derechos de autor y propiedad intelectual, privacidad y protección de datos personales y demás relacionados con la seguridad de la información.

14.1.1 Derechos de Autor y Propiedad Intelectual

La CIAC mediante la Gestión TIC’s propenderá porque el software instalado en los recursos tecnológicos cumpla con los derechos de autor y propiedad intelectual o que sea de libre distribución y uso.

Para el cumplimiento de los derechos de autor y propiedad intelectual se deben seguir las siguientes directrices:

- No instalar y/o duplicar software sin los derechos de uso o derechos de autor.
- El software utilizado debe contar con las licencias de uso requeridas, certificando así su autenticidad y legalidad

14.1.2 Privacidad y Protección de Datos Personales

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Corporación propende por la protección de los datos personales de sus clientes, proveedores y demás terceros de los cuales reciba y administre información.

Se establecen los términos, condiciones y finalidades para las cuales la Corporación, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, trata la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la CIAC S.A., hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Corporación exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, busca proteger la privacidad de la información personal de sus colaboradores, estableciendo los controles necesarios para preservar aquella información que la Corporación, conozca y almacene de ellos, velando porque tal información sea utilizada únicamente para funciones propias de la misma y no sea publicada, revelada o entregada a colaboradores o terceras partes sin autorización.

La CIAC tendrá presente, en todo momento, que los datos personales son propiedad de las personas a las que se refieren y que sólo ellas pueden decidir sobre los mismos. En este sentido, hará uso de ellos sólo para aquellas finalidades para las que se encuentra facultado debidamente, y respetando en todo caso la normatividad vigente sobre protección de datos personales y lo contemplado en la Resolución N° 168 de 17 de noviembre de 2016 - Por la cual se establece la política para el tratamiento de datos personales en la Corporación de la Industria Aeronáutica Colombiana S.A. - CIAC S.A.

Para el cumplimiento de la privacidad y protección de datos personales se deben seguir las siguientes directrices:

- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
- Obtener la autorización según lo establecido en la Política para el Tratamiento de Datos Personales (Resolución N° 168 de 17 de noviembre de 2016), con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir tales datos personales en el desarrollo de las actividades de la Corporación.
- Hay que asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a tales datos.
- Establecer condiciones contractuales y de seguridad con las entidades vinculadas o aliadas delegadas para el tratamiento de los datos personales.
- Acoger las directrices técnicas y procedimientos establecidos para el intercambio de datos con terceros delegados para el tratamiento de datos personales
- Acoger las directrices técnicas y procedimientos establecidos para enviar a los clientes, proveedores y terceros, mensajes a través de correo electrónico y/o mensajes de texto.
- Establecer controles para el tratamiento y protección de los datos personales de funcionarios, colaboradores, proveedores, clientes y demás terceros de los cuales reciba y administre información.
- Gestión TIC's deberá garantizar la protección de la información personal almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida de la información bajo su dominio.

14.2 Revisiones de Seguridad y Privacidad de la Información

Las políticas establecidas en el Manual de Seguridad y Privacidad de la Información serán revisadas una vez al año y/o cuando la aplicabilidad de estas cambie o por nuevas disposiciones legales que apliquen para asegurar su eficiencia y efectividad. La Gestión TIC’s con previa aprobación de la Alta Dirección tendrá la potestad de realizar estas modificaciones, las cuales se socializarán a todo el personal y partes interesadas por los medios que se consideren pertinentes.

14.3 Sanciones

Las políticas establecidas en el presente manual instituyen y afianzan la cultura de seguridad de la información entre los funcionarios, colaboradores, contratistas, pasantes, terceros y demás partes interesadas, por lo tanto, el incumplimiento de estas ameritará acciones correspondientes antes los organismos pertinentes.

Se consideran como violaciones graves a las políticas y directrices de la Seguridad y Privacidad de la Información:

- Divulgación no autorizada de información corporativa o de terceras partes cuya responsabilidad de no difusión esté a cargo de la Corporación y se clasifique como información Reservada o clasificada.
- Acciones que puedan exponer a la Corporación a la pérdida de imagen y/o negocios.
- Alteración a la información sensible de la Corporación.
- Hurto de hardware.
- Uso de información, equipos, software u otros recursos tecnológicos para propósitos ilícitos o violación a los reglamentos internos de la Corporación.
- Instalación de programas o aplicativos no autorizados sin el debido licenciamiento a nombre de la CIAC.

Se realizará un reporte a la Alta Dirección informando el incumplimiento a las políticas y directrices de seguridad y privacidad de la información para que se tomen las medidas correspondientes de acuerdo con los hallazgos encontrados y la gravedad de la falta.