Contenido

1. OBJETIVO

Establecer y recopilar las Políticas de Seguridad y Privacidad de la Información, Seguridad Digital y Ciberseguridad, al igual que definir los lineamientos frente al uso y manejo de la información en la Corporación de la Industria Aeronáutica Colombiana – CIAC, con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información, dando cumplimiento a los requisitos legales y reglamentarios.

2. DOCUMENTOS DE REFERENCIA

- Gobierno Digital
- Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC
- Estándar Internacional de Seguridad BASC 6.0.1
- Norma ISO IEC 27001:2013
- Roles y Responsabilidades Modelo de Seguridad y Privacidad de la Información - MINTIC
- Ley 2191 de 2022 – “Por medio de la cual se regula la desconexión laboral - ley de desconexión laboral”
- Resolución No. 013 de 2023 - "Por medio de la cual se adopta la política para el tratamiento de datos personales, se designa y establecen las competencias del oficial de datos personales de la Corporación de la Industria Aeronáutica Colombiana S.A."
- Resolución 7870 de 2022 – “Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.”
- Resolución 1519 de 2020 – “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.”
- POL-1-01-009 Política de Seguridad de la Información
- POL-1-01-013 Política Administración de licencias y usuarios SAP (ERP, SECESSFACTORS Y PAYROLL)

3. JUSTIFICACIÓN

Es necesario definir y recopilar en un documento las Políticas de Seguridad y Privacidad de la Información, Seguridad Digital y Ciberseguridad, al igual que definir los lineamientos frente al uso y manejo de la información en la Corporación de la Industria Aeronáutica Colombiana – CIAC, con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información, dando cumplimiento a los requisitos legales y reglamentarios.

4. ALCANCE

Las políticas establecidas en este manual aplican para los funcionarios, contratistas, pasantes, proveedores y terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten información y/o accedan a los activos de información de la Corporación de la Industria Aeronáutica Colombiana - CIAC S.A.

5. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y Recursos: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANS: Acuerdos de Nivel de Servicio:

Autenticidad: Seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad. (ISO/IEC 27000).

Ciberdelincuente: Persona que busca sacar beneficio de los problemas o fallos de seguridad encontrados en programas, servicios, plataformas o herramientas, utilizando distintas técnicas como la ingeniería social o el malware (https://www.incibe.es/aprendeciberseguridad/)

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados. (Resolución 7870 de 2022)

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. (www.ticportal.es/glosario-tic)

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

Directriz: Instrucción o norma que ha de seguirse en la ejecución de algo (RAE)

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 (Glosario (mintic.gov.co))

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

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. (Glosario MinTic)

Mesa de Ayuda: Herramienta destinada como único contacto entre los usuarios y Gestión TIC's para la atención de requerimientos.

No Repudio: Servicio que tiene como objetivo evitar que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red, garantizando la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción si ha tenido lugar. (https://colombiatic.mintic.gov.co)

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

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.

Personal en Comisión: Colaboradores que asisten como representantes de la CIAC a comités, reuniones, conferencias, seminarios, talleres, ferias u otros eventos relacionados con sus funciones u obligaciones dentro o fuera del país.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico. (Guía No. 2 Seguridad y Privacidad de la Información MinTic)

Propietario de la Información: 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. (Guía No. 5 Seguridad y Privacidad de la Información MinTic)

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 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. (Modelo de Seguridad y Privacidad de la Información - MinTIC)

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 (RAE)

Ticket: Número de proceso o caso registrado en la herramienta destinada como mesa de ayuda para la atención de requerimientos de Gestión TIC's

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La política está relacionada en el documento Política de Seguridad de la Información con el código POL-1-01-009 en Isolución o en el sitio web en Gobierno Digital/Transparencia

7. ROLES Y RESPONSABILIDADES

Las responsabilidades referentes a la seguridad y privacidad de la información no son solamente de Gestión TIC's, sino que son distribuidas dentro de toda la Corporación. A continuación, se definen los roles y responsabilidades para la seguridad y privacidad de la información:

Alta Dirección:

- Acompañar e impulsar los proyectos de seguridad de la información, seguridad digital y ciberseguridad.
- Articular los esfuerzos instituciones, recursos y estrategias para asegurar la implementación, sostenibilidad y mejora de la seguridad de la información, seguridad digital y ciberseguridad en la Corporación.
- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad de la información, seguridad digital y ciberseguridad.

- Promover una cultura de seguridad y privacidad de la seguridad de la información.

Comité Institucional de Gestión y Desempeño

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
- Realizar seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad digital y de privacidad de la información.
- Aprobar acciones y mejoras en la implementación del Modelo de Seguridad y Privacidad de la Información.
- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad digital y privacidad de la información.

Grupo Gestión TIC's

- Desarrollar políticas y controles de seguridad de la información, seguridad digital y ciberseguridad que garanticen la integridad, confidencialidad, disponibilidad y privacidad de los activos de información.
- Alinear la estrategia de seguridad de la información, seguridad digital y ciberseguridad con los objetivos de la Corporación.
- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad de la información y ciberseguridad.
- Identificar, analizar y reportar los incidentes de seguridad de la información, seguridad digital y ciberseguridad.
- Revisar y gestionar los controles de seguridad de la información y seguridad digital.
- Brindar acompañamiento a los procesos de la Corporación en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Custodiar los sistemas de información que están bajo su administración
- Elaborar campañas de sensibilización sobre ciberseguridad

Grupo Asesor Jurídico

- Identificar los aspectos legales referentes al cumplimiento de la seguridad de la información, seguridad digital y ciberseguridad.
- Brindar asesoría a los proceso en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

Gestión de Talento Humano

- Controlar y salvaguardar la información de datos personales del personal de la Corporación, en concordancia con la normatividad vigente.
- Realizar la gestión de vinculación, capacitación, desvinculación del personal dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

Coordinador, jefe o director de área, oficina o grupo

- Identificar y realizar el inventario de los activos de información y los riesgos cibernéticos asociados.
- Realizar el análisis y tratamiento de riesgos de ciberseguridad de sus procesos.
- Aplicar los controles establecidos para preservar la integridad, disponibilidad, confidencialidad y privacidad de la información.
- Determinar los criterios y niveles de acceso de la información, así como de los sistemas de información que apoyan los procesos y áreas que lidera, por ser el propietario de la información.

Usuarios

- Cumplir las políticas y controles establecidos para proteger la integridad, disponibilidad, confidencialidad y privacidad de la información.
- Comunicar cualquier incidente de seguridad de la información, seguridad digital y ciberseguridad.
- Garantizar la confidencialidad de la información que reciba, genere o procese la Corporación.

8. NIVELES DE ACUERDOS DE SERVICIO

Gestión TIC's utiliza como único medio de contacto con los usuarios, el Ticket registrado en la herramienta destinada como mesa de ayuda y establece los siguientes tiempos estimados de respuesta, teniendo en cuenta el nivel de impacto una vez analizado el requerimiento solicitado y el orden de llegada de este.

NIVEL IMPACTO	DESCRIPCIÓN	DEFINICIÓN	SERVICIO	TIEMPO ESTIMADO DE RESPUESTA
1	Crítico	Cuando ocurre un evento inesperado que afecta de manera	• Infraestructura crítica TI • Internet • Correo corporativo	Durante las próximas 2 horas hábiles de haber recibido el Ticket en la

		masiva el uso total del servicio.	• Sistemas de información (DataDoc, SAP, Isolución, entre otros.)	herramienta destinada como mesa de ayuda o por monitoreo del servicio.
2	Alto	Cuando ocurre una pérdida severa en el funcionamiento de un servicio o recurso tecnológico e impide de manera parcial su utilización.	• Servicio de impresión. • Sistemas de información (DataDoc, SAP. Isolución, entre otros.)	Durante las próximas 8 horas hábiles de haber recibido el Ticket en la herramienta destinada como mesa de ayuda
3	Normal	Cuando ocurre una situación que dificulta el correcto funcionamiento de un servicio o recurso tecnológico, pero puede continuar con su utilización.	• Soporte de red (Puntos de red, WIFI e Internet) • Acceso a VPN • Usuario y Contraseña (Equipo de cómputo, DataDoc, correo, SAP, SuccessFactor) • Acceso a páginas web • Soporte de Hardware • Soporte de Software • Soporte Gestor Documental • Soporte Office 365 (Aplicaciones Office, Teams, OneDrive, Sharepoint) • Carpetas compartidas	Durante las próximas 24 horas hábiles de haber recibido el Ticket en la herramienta destinada como mesa de ayuda

			• Modificaciones Página Web • Novedades Personal (Vacaciones, Incapacidades, Vinculación y Terminación laboral)	
4	Bajo	Cuando no existe la detención en la operación del servicio o recurso tecnológico, y cuando se requiere realizar una tarea que se desempeña de forma programa.	• Solicitud de sonido y video (Parlantes, micrófonos, Video Beam) • Solicitud de Tóner • Fondo de pantalla. • Custodia de equipos o parte	Durante las próximas 48 horas hábiles de haber recibido el Ticket en la herramienta destinada como mesa de ayuda

En caso de que la herramienta dispuesta para la Mesa de Ayuda no esté disponible, se recibirán solicitudes por medio de correo electrónico con los soportes correspondientes y posteriormente realizar la legalización mediante Ticket.

Para los casos críticos que no esté disponible el correo electrónico y/o el servicio de Internet, se recibirá la solicitud verbal y posteriormente se legalizará mediante Ticket.

9. POLÍTICA DE SEGURIDAD DE LOS DISPOSITIVOS MÓVILES

Gestión TIC's establece las directrices para mitigar los riesgos generados por el uso de dispositivos móviles como computadores portátiles, tabletas, teléfonos inteligentes o smartphones, entre otros, que hagan uso de los servicios de la Corporación de la Industria Aeronáutica Colombiana - CIAC

- 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 corporativos no deben dejarse desatendidos o expuestos en espacios públicos, con el fin de prevenir posibles accesos no autorizados por terceros.
- 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.
- Es responsabilidad del usuario del dispositivo móvil generar una copia de respaldo de la información almacenada, por lo tanto, debe realizar respaldos regulares para garantizar la recuperación de datos en caso de pérdida o daño del dispositivo.
- Los dispositivos móviles no pueden ser retirados de las instalaciones de CIAC, sin previa autorización de la Gerencia o Subgerencia, igualmente, se debe realizar el proceso de retiro de elementos que esté establecido.
- El usuario debe utilizar los dispositivos móviles corporativos solamente para las funciones asignadas o el cumplimiento de los objetivos corporativos.
- El usuario no debe hacer uso de los dispositivos móviles en redes inalámbricas públicas, con el fin de prevenir ataques y accesos no autorizados.
- Gestión TIC’s instala un programa de antivirus en los dispositivos móviles corporativos teniendo en cuenta las características de cada dispositivo.
- Los dispositivos móviles que no pertenezcan al inventario de activos fijos de la Corporación y requieran conexión a Internet, deben ser registrados en el formulario dispuesto por Gestión TIC’s para realizar el registro de la MAC del dispositivo.
- No se permite el uso de dispositivos móviles personales que no estén autorizados y que tengan intención de sustraer información de la Corporación.
- Para los dispositivos móviles personales no se proporciona conexión a la infraestructura tecnológica corporativa, solamente acceso a la WIFI de invitados.

10. SEGURIDAD DE LOS RECURSOS HUMANOS

Gestión de Talento Humano con el apoyo de Gestión TIC's desplegarán esfuerzos para que los colaboradores, pasantes y terceros conozcan sus responsabilidades frente a la seguridad de la información, seguridad digital y ciberseguridad, con el fin de reducir el riesgo por hurto de medios informáticos, acceso abusivo a los sistemas informáticos, daño informático y de aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

Se establecen las siguientes directrices:

- Gestión de Talento Humano debe reportar todas las novedades de ingreso y retiro de personal de manera inmediata a la Gestión TIC's, al igual que vacaciones, licencias no remuneradas, incapacidades o cualquier otra novedad con el fin de gestionar las acciones relacionadas con la seguridad de la información.
- Gestión de Talento Humano debe incluir en los programas de inducción y de reinducción el tema de seguridad de la información, asegurando que los colaboradores conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos.
- Los colaboradores que se desvinculen deben hacer entrega de la información que manejan al jefe del área y realizar el proceso definido para la entrega de los activos fijos que tenga a cargo.

11. 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.

12. POLÍTICA DE USO DE LOS RECURSOS TECNOLÓGICOS

Los recursos tecnológicos de la Corporación de la Industria Aeronáutica Colombiana - CIAC, son herramientas de apoyo para el desempeño de las funciones y responsabilidades labores de los colaboradores, por lo tanto, deben hacer un uso adecuado y eficiente de estos y cumplir con las siguientes directrices:

- Los bienes de cómputo suministrados por CIAC, se emplearán únicamente para las funciones asignadas o el cumplimiento de los objetivos corporativos y bajo la responsabilidad del colaborador al cual han sido asignados, por lo tanto, no deben utilizarse para fines personales.
- Solo está permitido el uso de software licenciado por la Corporación y el que sin requerir licencia sea expresamente autorizado por Gestión TIC's
- Gestión TIC´s es la dependencia autorizada para la administración del software o para autorizar su administración a otra dependencia, el cual no debe ser copiado, ni suministrado a terceros, ni utilizado para fines personales.
- Es responsabilidad de los colaboradores realizar y mantener copias de seguridad de su información y entregarla al finalizar la vinculación con la Corporación al coordinador, jefe o director de área, oficina o grupo. Esto también aplica para cuando se hace cambio de cargo u oficina.

- Está prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles, discos virtuales de red o almacenamiento en la nube, archivos de vídeo, música y fotos que no sean de carácter corporativo o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y por consiguiente pérdida de la integridad de ésta.
- Los colaboradores deben utilizar las herramientas tecnológicas proporcionadas por Gestión TIC's para gestionar la información digital de la Corporación.
- Los equipos de cómputo y periféricos deben quedar apagados al terminar la jornada laboral o cada vez que el personal no se encuentre en la oficina o durante la noche.
- Todos los días a las 21:00 horas se apagan automáticamente los computadores, con el fin de contribuir a la disminución del gasto energético innecesario y prolongar la vida útil de los equipos. Las personas o dependencias que por algún motivo requieran trabajar después de la hora establecida, deben enviar un correo a gtics@ciac.gov.co con la lista de equipos y la debida justificación
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, a excepción de los casos autorizados expresamente por Gestión Administrativa.
- 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.
- Gestión TIC's implementa mecanismos de gestión y monitoreo permanente a la infraestructura TI de los servicios utilizados, con el fin de protegerlas de amenazas físicas y digitales.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los recursos tecnológicos como destapar, agregar, desconectar, revisar, instalar, configurar o reparar los componentes, son las designadas por la Gestión TIC’s para realizar esta labor.
- La pérdida o daño de recursos tecnológicos o de alguno de sus componentes, debe ser reportado de forma inmediata al área de Activos Fijos del Grupo de Gestión Administrativa y al Grupo de Gestión TIC's por parte del colaborador que tiene asignado el recurso y seguir el procedimiento establecido para este tipo de siniestros.
- Para retirar cualquier recurso tecnológico de las instalaciones de la CIAC, se debe diligenciar el F-2-04-067 que se encuentra en Isolución y seguir el proceso establecido.

- Cualquier colaborador debe reportar de forma inmediata al Grupo de Gestión Administrativa y al Grupo de Gestión TIC´s, 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, peligro de incendio o cualquier tipo de evento que se prevea puede ocasionar daño a cualquier recurso tecnológico de la Corporación.
- Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información digital debe ser reportado a la mayor brevedad al Grupo de Gestión TIC's.

13. POLÍTICA DE USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de apoyo a la ejecución de las funciones y obligaciones contractuales de los colaboradores, por lo cual se deben seguir las siguientes directrices para su uso:

- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información corporativa en la entidad es el asignado por Gestión TIC's, con el dominio @ciac.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando cualquier tipo de ataque cibernético.
- Para la creación de cuentas de correo electrónico, se siguen las directrices establecidas en el numeral *18.1 Gestión de usuarios* y se crean de acuerdo con la disponibilidad de licenciamiento del correo.
- El nombre de la cuenta se genera con la inicial del primer nombre, punto y el primer apellido, es decir a.apellido@ciac.gov.co, en caso de repetirse se agrega la inicial del segundo apellido, es decir a.apellidoa@ciac.gov.co
- La cuenta de correo electrónico corporativo asignada es de carácter individual, por lo tanto, el usuario al que se le asigna es el responsable de su administración y no debe permitir que otro colaborador envíe correos utilizando su cuenta.
- El servicio de correo electrónico corporativo debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, por consiguiente, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro fin ajeno a los propósitos de la Corporación.
- En cumplimiento a la iniciativa corporativa del uso aceptable del papel y la eficiencia administrativa, se debe priorizar el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
- Se prohíbe el envío de correos masivos internos o externos, con excepción de los enviados a los grupos específicos dentro de la Corporación, por parte de los coordinadores, jefes o directores de área, oficina o grupo y las personas que por la

naturaleza de su cargo requieran esta función. Se restringe a máximo dos (2) personas por área, oficina o grupo para el envío a los grupos establecidos.

- Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe reportarse inmediatamente a Gestión TIC's mediante la opción de reportar mensaje habilitada en el buzo o al correo gtics@ciac.gov.co para bloquearse y evitar su propagación.
- La cuenta de correo corporativo no debe ser revelada en páginas o sitios publicitario, de comercio electrónico, deportivos o cualquier otra ajena a los fines de la Corporación.
- Está prohibido el uso del correo corporativo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atentan contra la integridad moral y/o buena imagen de las personas o institucionales, las leyes vigentes, o directrices establecidas.
- Está expresamente prohibido distribuir, copiar, reenviar información de propiedad de la Corporación a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
- 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 de transporte de 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 fines corporativos.
- Los correos con dirección de Gmail, Hotmail, Yahoo, entre otros, están sujetos a la verificación del contenido, tanto para envío o recepción por parte de Gestión TIC's para su aprobación o rechazo.
- Gestión se reserva el derecho de monitorear los accesos y el uso de los buzones de correo corporativo de los colaboradores, adicionalmente podrá limitar el acceso temporal o definitivo cuando sospeche o encuentre vulnerabilidades en la cuenta de correo.
- Gestión TIC's podrá realizar copias de seguridad del correo electrónico corporativo en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo, previa solicitud expresa de la Gerencia, Subgerencia, Control Interno o el coordinador, jefe o director de área, oficina o grupo.
- Para el personal en comisión debe informar mediante Ticket en la herramienta destinada como mesa de ayuda que requiere hacer uso del correo corporativo para permitir su acceso, adicionalmente se deben seguir los lineamientos establecidos en el numeral *17.1.2 Usuario de personal en comisión.*

14. POLÍTICA DE USO DE INTERNET

Gestión TIC's establece políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, y supervisa el uso y acceso del servicio de internet verificando que esté siendo usado apropiadamente para el cumplimiento de las funciones y objetivos corporativos, y será responsabilidad de los colaboradores seguir las siguientes directrices:

- No se permite enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atente contra la integridad moral de las personas o de las instituciones, las leyes vigentes, o directrices establecidas.
- No se permite acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por 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.
- No se permite propagar intencionalmente virus o cualquier tipo de código malicioso.
- En caso de requerirse el acceso a un sitio web específico se debe realizar la solicitud mediante Ticket en la herramienta dispuesta como Mesa de Ayuda, justificando la necesidad para la verificación, aprobación y habilitación por parte de Gestión TIC's.
- Gestión TIC's se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, así como limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivo y cualquier otro uso ajeno a los fines corporativos.

15. POLÍTICA DE USO DE REDES SOCIALES

Se establecen las siguientes directrices para el uso de las redes sociales por parte de los usuarios autorizados

- Las redes sociales de carácter corporativo no deben ser abiertas a nombre propio de colaboradores sino de la entidad
- El colaborador responsable del manejo de las redes sociales corporativas debe garantizar el uso adecuado de estas.
- Las redes sociales de carácter corporativo son controladas por el área de Comunicaciones, con el fin de contar con los niveles de protección adecuados para su uso correcto y seguro.

- No utilizar la contraseña de una red social en otros sitios de internet y nunca compartirla.
- Evitar utilizar computadores públicos para ingresar en las redes sociales corporativas.
- No se debe utilizar el nombre de CIAC en las redes sociales para difamar o afectar la imagen y/o reputación de los seguidores cuando respondan comentarios en contra de los principios y valores de la Corporación.
- No se recomienda la administración de las redes sociales en dispositivos móviles personales.

16. POLÍTICA DE USO DE LOS SISTEMAS O HERRAMIENTAS TECNOLÓGICAS

Todos los colaboradores que laboran en la Corporación de la Industria Colombiana – CIAC, son responsables de la protección de la información que acceden y procesas, así como de evitar su pérdida, alteración, destrucción y uso indebido, y deberán seguir las siguientes directrices:

- El usuario y contraseña asignado para el acceso a los sistemas y/o herramientas tecnológicas es de carácter individual e intransferible, por lo tanto, el colaborador al que se le asigna es el responsable de su administración y no debe permitir que otra persona utilice sus datos de acceso.
- Es responsabilidad del colaborador realizar el cambio periódico de la contraseña para el acceso a los sistemas o herramientas tecnológicas asignadas, teniendo en cuenta las directrices establecidas en la política de Control de Accesos.
- Todo colaborador es el responsable de los registros y modificaciones de información que se realicen a nombre de su cuenta de usuario.
- En ausencia del colaborador, el acceso a la estación de trabajo será bloqueada, con el fin de evitar exposición de la información y el acceso a terceros que puedan generar daño, alteración o uso indebido, y/o suplantación de identidad.

17. POLÍTICA DE MEDIOS DE ALMACENAMIENTO

La Corporación de la Industria Colombiana – CIAC establece directrices para evitar la divulgación, modificación, retiro o destrucción no autorizados de información almacenada en los diferentes medios, protegiendo la confidencialidad, integridad y disponibilidad de esta.

17.1 MEDIOS DE ALMACENAMIENTO REMOVIBLE

Se establecen las siguientes directrices para los medios de almacenamiento removible:

- 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.

17.2 MEDIO DE ALMACENAMIENTO EN LA NUBE

Se establecen las siguientes directrices para el almacenamiento en la nube:

- La Corporación de la Industria Colombiana – 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.
- Está prohibido el almacenamiento de archivos de vídeo, música y fotos que no sean de carácter corporativo o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- 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.

17.3 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.

Está prohibido el almacenamiento de archivos de vídeo, música y fotos que no sean de carácter corporativo o que atenten contra los derechos de autor o propiedad intelectual de los mismos.

18. POLÍTICA DE CONTROL DE ACCESO

La Corporación de la Industria Colombiana – CIAC asegura y limita el acceso a las redes de datos, recursos tecnológicos y sistemas de información mediante privilegios para que los usuarios tengan solamente el acceso autorizado, con el fin de proteger la integridad, disponibilidad y confidencialidad de la información.

18.1 GESTIÓN DE USUARIOS

Gestión TIC's proporciona el acceso a los recursos y servicios tecnológicos como usuario en el Directorio Activo, equipo de cómputo, correo electrónico corporativo, gestor documental DataDoc y al ERP SAP, siempre utilizando el principio del mínimo privilegio necesario para la realización de las funciones o el cumplimiento de los objetivos misionales de la Corporación.

18.1.1 Usuarios de Recursos y Servicios Tecnológicos

Se establecen las siguientes directrices para un acceso controlado a los recursos y servicios tecnológicos (Usuario en el Directorio Activo, Equipo de Cómputo, Correo Electrónico Corporativo y Gestor Documental):

- Gestión de Talento Humano debe reportar de manera inmediata a Gestión TIC's todas las novedades de personal como ingreso, vacaciones, licencias no remuneradas, incapacidades, retiros o cualquier otra novedad que implique asignar o suspender los accesos a los recursos y servicios tecnológicos durante el período establecido.
- Es responsabilidad del coordinador, jefe o director de área, oficina o grupo gestionar los permisos para cada usuario mediante Ticket en la herramienta destinada como Mesa de Ayuda, como control de autorización de los perfiles.
- Toda creación, modificación, activación o cancelación de accesos a los recursos y servicios tecnológicos debe realizarse mediante Ticket en la herramienta destinada como Mesa de Ayuda.
- En caso de que la herramienta dispuesta para la Mesa de Ayuda no esté disponible, se recibirán solicitudes por medio de correo electrónico con los soportes correspondientes para la gestión de acceso a usuarios y posteriormente realizar la legalización mediante Ticket.
- Para acceso a usuarios nuevos y cambios de cargo, el Ticket debe contener el *acta de equipos fijos*, el *nombre completo, cédula, cargo, teléfono, activo fijo en el cual va a trabajar, tipo de contrato, fecha inicial y fecha final de vinculación, fecha en la que asistió a la inducción corporativa general de CIAC.*

- Para la creación de accesos es requisito haber tomado la inducción, por lo tanto, en caso de no haber asistido a la inducción corporativa general o la asistencia a esta es una fecha posterior, se debe coordinar con Gestión TIC's para recibir la inducción de ciberseguridad.
- Se aplica el principio de mínimo privilegio, por lo tanto, se asigna perfil con limitaciones para la navegación en internet acorde al cumplimiento objetivos misionales de la Corporación y con restricción para instalar cualquier tipo de software en los equipos de cómputo.
- El único personal autorizado con perfil de administrador son los colaboradores (Coordinador, profesional de infraestructura y operaciones) de Gestión TIC's, que cuentan con privilegios elevados para instalación de software, gestión y monitoreo de servidores, aplicaciones, redes, equipos de cómputo, impresoras y sistemas operativos.
- Las contraseñas deben cumplir los siguientes parámetros y cambiarse antes de que la cuenta expire:
    - Longitud mínima de 9 caracteres
    - Contener caracteres alfanuméricos (letras y números)
    - Incluir mínimo una letra mayúscula, un número, un carácter especial.
    - Longitud máxima de 15 caracteres.
    - La contraseña temporal que se asigna inicialmente debe cambiarse en el primer inicio de sesión.
    - Cambiarse cada 45 días.
- En caso de retiro de personal, a parte del reporte de Gestión de Talento Humano, el coordinador, jefe o director de área, oficina o grupo, debe gestionar la cancelación de accesos a los recursos y servicios tecnológicos e informar el recibido de la copia de seguridad de la información del usuario, mediante Ticket en la herramienta destinada como Mesa de Ayuda, para que el colaborador que se retira registre este número en el formato de paz y salvo.

18.1.2 Usuarios de Personal en Comisión

Se establecen las siguientes directrices cuando el personal tenga aprobado por parte de Subgerencia el desplazamiento para asistir a comités, reuniones, conferencias, seminarios, talleres, ferias u otros eventos relacionados con sus funciones u obligaciones dentro o fuera del país:

- El coordinador, jefe o director de área, oficina o grupo debe informar a Gestión TIC's mediante Ticket en la herramienta destinada como mesa de ayuda la siguiente información, con el fin de mantenerle los accesos a los recursos y herramientas tecnológicas que lleguen a necesitar en la comisión:

- Nombre completo del colaborador
- Fecha inicial y fecha final de la comisión
- Ubicación física de la comisión (Incluir ciudad y país o departamento)
- Lista detallada de los recursos y herramientas tecnológicas requeridos (Ejemplo: Acceso a sistemas internos, correo corporativo, software específico, dispositivos, entre otros)
- Si se requerirá acceso a datos confidenciales o sensibles y el uso de VPN
- Número de contacto en caso de que se presenten problemas técnicos, Gestión TIC's pueda comunicarse directamente.

- El Ticket debe realizarse mínimo dos (2) días antes para que Gestión TIC's revise la solicitud y evalúe los recursos y permisos necesarios.
- En caso de que la herramienta dispuesta para la Mesa de Ayuda no esté disponible, se recibirán solicitudes por medio de correo electrónico con los soportes correspondientes para la gestión de acceso a usuarios y posteriormente realizar la legalización mediante Ticket.
- Cuando se requiera algún desbloqueo o configuración especial, el Ticket debe ser aprobado por la Coordinación de Gestión TIC's.
- Se deben seguir las medidas de seguridad adecuadas como el uso de VPN.
- Una vez revisada la solicitud se informará que los recursos y herramientas tecnológicas estarán disponibles durante su comisión y que su acceso no será bloqueado por medidas de seguridad.
- Si no se realiza el requerimiento, los accesos a los recursos y herramientas tecnológicas pueden bloquearse y ser catalogados como intrusiones cibernéticas.

18.1.3 Usuarios ERP SAP

Se establecen las siguientes directrices para un acceso controlado al ERP SAP:

- Gestión de Talento Humano deberá reportar de manera inmediata a Gestión TIC's todas las novedades de personal como ingreso, vacaciones, licencias no remuneradas, incapacidades o cualquier otra novedad que implique asignar o suspender los accesos a los recursos y servicios tecnológicos durante el período establecido.
- Es responsabilidad del coordinador, jefe o director de área, oficina o grupo gestionar los permisos para cada usuario mediante Ticket en la herramienta destinada como Mesa de Ayuda, como control de autorización de los perfiles.

- Toda creación, modificación, activación o cancelación de accesos para el ERP SAP debe realizarse mediante Ticket en la herramienta destinada como Mesa de Ayuda.
- En caso de que la herramienta dispuesta para la Mesa de Ayuda no esté disponible, se recibirán solicitudes por medio de correo electrónico con los soportes correspondientes para la gestión de acceso a usuarios y posteriormente realizar la legalización mediante Ticket.
- 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.
- 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.
- Se aplica el principio de mínimo privilegio necesario para la realización de las funciones o el cumplimiento de los objetivos misionales de la Corporación.
- Se crean cuentas para cada usuario con el fin de determinar las responsables en la administración de estas y de acuerdo con la disponibilidad de licencias.
- El único personal autorizado con perfil de administrador son los colaboradores (Coordinador y la profesional Controller SAP) de Gestión TIC's, que cuentan con privilegios elevados para la administración del ERP.
- Las contraseñas deben cumplir los siguientes:
    - Longitud mínima de 8 caracteres
    - Contener caracteres alfanuméricos (letras y números)
    - Incluir mínimo una letra mayúscula, un número, un carácter especial.
    - Longitud máxima de 40 caracteres.
    - La contraseña temporal que se asigna inicialmente debe cambiarse en el primer inicio de sesión.
    - Cambiarse cada 30 días.
- Mensualmente o cada vez que se requiera, el Profesional Controller SAP verifica con los líderes funcionales de SAP que los roles y perfiles asignados correspondan a las funciones que realiza cada usuario, al igual que estén inactivos los usuarios del personal retirado y se actualiza la matriz de roles y perfiles.
- En caso de retiro de personal, a parte del reporte de Gestión de Talento Humano, el coordinador, jefe o director de área, oficina o grupo, debe gestionar la cancelación de accesos a los accesos de SAP, mediante Ticket en la herramienta destinada como Mesa de Ayuda, para que el colaborador que se retira registre este número en el formato de paz y salvo.

18.1.4 Usuarios SuccessFactors

Se establecen las siguientes directrices para un acceso controlado a SuccessFactors:

- La creación de usuarios para el personal de planta y militar la realiza Gestión de Talento Humano y para el personal temporal CECSA
- Para restablecer cuentas de usuario y contraseñas por bloqueo u olvido debe realizarse mediante Ticket en la herramienta destinada como Mesa de Ayuda.
- Las contraseñas deben cumplir los siguientes parámetros:
  - Longitud mínima de 8 caracteres
  - Contener caracteres alfanuméricos (letras y números)
  - Incluir mínimo una letra mayúscula, un número, un carácter especial.
  - Longitud máxima de 18 caracteres.
  - La contraseña temporal que se asigna inicialmente debe cambiarse en el primer inicio de sesión.
  - Cambiarse cada 30 días.
- En caso de retiro los usuarios de planta son inactivados por el Grupo de Talento Humano y para los usuarios temporales el CECSA.

18.1.5 Usuarios Isolución

La gestión de usuarios para el aplicativo Isolución debe realizarse con el equipo SIGCA de la Oficina de Planeación, Innovación y Desarrollo – OPLAI y se siguen las siguientes directrices:

- Las licencias son limitadas, por lo tanto, los usuarios están repartidos en todas las dependencias de la Corporación.
- Las contraseñas deben cumplir los siguientes parámetros:
  - Longitud mínima de 8 caracteres
  - Contener caracteres alfanuméricos (letras y números)
  - Incluir mínimo una letra mayúscula, un número, un carácter especial.
  - Cambiarse cada 90 días.

18.2 DERECHOS DE ACCESO PRIVILEGIADO

Gestión TIC restringe y controla la asignación y uso de derechos de acceso privilegiado a los recursos y servicios tecnológicos de la Corporación, velando porque sean operados y administrados en condiciones controladas y de seguridad, permitiendo el monitoreo de los usuarios administradores que poseen los más altos privilegios.

Se establecen las siguientes directrices para los accesos privilegiados:

- Otorgan los privilegios para administración de los recursos y servicios tecnológicos solo a aquellos colaboradores designados para estas funciones.
- Establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos y servicios tecnológicas.
- Restringir las conexiones remotas a los recursos tecnológicos, permitiendo únicamente el acceso a personal autorizado.
- Los usuarios o perfiles de usuario que traen por defecto los recursos y servicios tecnológicos deben renombrarse o suspenderse.
- Cambiar las contraseñas que traen por defecto los usuarios administradores de los recursos y servicios tecnológicos.
- Los equipos de cómputo deben estar configurados con restricciones para la instalación de programas y/o utilitarios que permitan acceso privilegiado a los recursos y servicios tecnológicos.
- Controlar que los usuarios finales de los recursos y servicios tecnológicos no tengas instalados en los equipos de cómputo programas y/o utilitarios que permitan tener acceso privilegiado a estos recursos y servicios.
- No utilizar software o herramientas tecnológicas que permitan evadir los controles de seguridad establecidos para los recursos y servicios tecnológicos.

18.3 ACCESO A SISTEMAS Y APLICACIONES

Se establecen las siguientes directrices para el acceso a sistemas y aplicaciones:

- El coordinador, jefe o director de área, oficina o grupo como propietarios de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, deben velar por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos.
- El coordinador, jefe o director de área, oficina o grupo son los responsables de la administración y gestión de los sistemas de información o aplicaciones externas y deben velar por la confidencialidad e integridad de la información de cada sistema o aplicación a cargo.
- Gestión TIC’s lleva un consolidado de las plataformas externas que se manejan en la Corporación, pero cada grupo es el responsable de garantizar la confidencialidad e integridad de la información de cada sistema o aplicación a cargo.

18.4 ACCESO A REDES Y SERVICIOS DE RED

Gestión TIC's como responsable de las redes de datos y los recursos de red de la Corporación, procura que estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Los colaboradores de la Corporación de la Industria Aeronáutica Colombiana – CIAC, deben cumplir con las siguientes responsabilidades para el acceso a redes y servicios 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.
- Todo acceso a la red de la entidad mediante recursos tecnológicos no corporativos debe ser informado y autorizado.
- Cuando se requiere hacer reubicación física de equipos de cómputo, debe realizarse la solicitud mediante Ticket en herramienta destinada como Mesa de Ayuda, para la configuración de los puertos y accesos a la red, de lo contrario, estos se bloquean automáticamente debido a que están habilitados para un equipo específico.
- 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.
- Para el acceso remoto al aplicativo Isolución, se dispone de VPN Forticlient que garantiza el acceso seguro. Se prohíbe el uso de aplicaciones de conexiones remotas que no estén autorizadas por Gestión TIC's. Para la instalación y configuración de VPN consulte en Isolución el instructivo con el código I-7-00-021.
- Para cualquier dispositivo que requiera conectarse mediante WIFI, debe ser registrado en la herramienta dispuesta por GTIC's anotando la MAC del equipo, de lo contrario no tendrá acceso al servicio, esto como control adicional a la contraseña de la red inalámbrica.

18.5 GESTIÓN DE CONTRASEÑAS

Gestión TIC's establece las buenas prácticas para el uso de contraseñas seguras, con el fin de evitar el acceso no autorizado a los sistemas, aplicaciones y herramientas informáticas, por lo tanto, todos los colaboradores deben seguir las siguientes directrices:

- No utilizar las contraseñas por defecto, se debe cambiar las contraseñas en el primer inicio de sesión para el acceso a los sistemas, aplicaciones y herramientas informáticas.
- No utilizar contraseñas vulnerables como “12345”, “123456789”, “abcd”, “password”, “contraseña”, “agosto*2023” o relacionadas con CIAC.
- No utilizar palabras obvias como el nombre, cargo o fechas de cumpleaños.
- No dejar las contraseñas anotadas en lugares inseguros, como papeles, notas o post it adheridas a los equipos.
- Cambiar las contraseñas periódicamente y no compartirlas con nadie.
- Utilizar la verificación en dos pasos, siempre que sea posible.
- Las contraseñas deben ser robustas y fácil de recordar. La longitud mínima recomendada es de 10 caracteres
- Para crear una contraseña segura se recomienda pensar en una frase o simplemente una 2 0 3 palabras que solo usted conozca, alternar mayúsculas y minúsculas, sustituir letras por números y añadir caracteres especiales, por ejemplo: M1Cu3n74S3gur4

19. POLITICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

La Corporación de la Industria Aeronáutica Colombiana - CIAC evita 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 controla las amenazas físicas tanto internas como externas, y las condiciones medioambientales que pongan en riesgo la infraestructura tecnológica y afecten la confidencialidad, integridad y disponibilidad de la información.

19.1 ÁREAS SEGURAS

Se establecen las siguientes directrices para las áreas seguras, con el fin de prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Corporación:

- El Data Center principal, sus alternos y los centros de cableado deben permanecer bajo llave y solo el personal autorizado puede tener acceso.
- 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.
- Modificar y prohibir de manera inmediata los privilegios de acceso físico al Data Center principal, sus alternos y los centros de cableado, en los eventos de desvinculación o cambio en las labores de un colaborador con estos privilegios.
- Gestión TIC's debe verificar que el Data Center principal, sus alternos y los centros de cableado que están bajo su coordinación se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- Gestión Administrativa deben proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en los Centros de datos.
- El cableado debe estar protegido con el fin de disminuir las intercepciones o daños.
- Los recursos de la plataforma tecnológica de la Corporación ubicados en los Centro de datos deben estar protegidos contra fallas o interrupciones eléctricas.
- Las labores de mantenimiento de redes eléctricas, de voz y de datos deben ser realizadas por personal idóneo, autorizado e identificado.
- El personal tanto de la Corporación y el provisto por terceras partes no deben ingresar a las áreas a las cuales no tengan autorización
- Se seguirán los lineamientos para el control de acceso y seguridad física establecidos por Seguridad Aeroportuaria e Instalaciones del Grupo de Gestión Administrativa y Financiera.

19.2 SEGURIDAD DE LOS EQUIPOS

Se establecen las siguientes directrices para la seguridad de los equipos, con el fin de prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Corporación:

- 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 colaboradores están autorizados solo para ingresar al equipo de cómputo que tienen asignado, en caso de requerir acceder a un equipo diferente al asignado, el responsable de dicho equipo debe colocar un Ticket mediante la herramienta destinada como mesa de ayuda, solicitando el acceso del usuario con la debida justificación y adjuntando el acta de activos fijos.

- El colaborador no debe realizar ninguna alteración física de los componentes de los equipos de cómputo.
- En caso de presentarse alguna falla de Hardware o Software en un equipo, el colaborador responsable debe informar a Gestión TIC's mediante un Ticket en la herramienta destinada como mesa de ayuda para brindar el respectivo soporte.
- Se deben realizar mantenimientos preventivos y correctivos a los equipos de cómputo y a los servidores mínimo una vez al año para asegurar la disponibilidad e integridad de estos.

20. POLÍTICA DE ESCRITORIO, PANTALLA LIMPIA Y PERIFÉRICOS DESPEJADOS

Todo el personal que labore en la Corporación de la Industria Aeronáutica Colombiana – CIAC, debe mantener el escritorio, la pantalla limpia y los periféricos despejados, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información, y deberán seguir las siguientes directrices:

- Todos los usuarios deben bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que lo bloqueó.
- En los equipos de cómputo por inactividad, la sesión se bloquea cada 3 minutos como medida de control en equipos desatendidos.
- Para las sesiones remotas de los servidores debe configurarse el cierre de sesión automático por inactiva.
- Se deben tomar las medidas de seguridad necesarias en el uso de las contraseñas para evitar que estas sean conocidas tanto por el personal interno o externo a la Corporación.
- No dejar las contraseñas anotas en lugares inseguros, como papeles, notas o post it adheridas a los equipos.
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, dejar los medios que contengan información crítica protegida bajo llave.
- Todos los colaboradores deben mantener su escritorio libre de información propia de la Corporación que pueda ser utilizada o copiada por personal que no tenga autorización para su uso o conocimiento.
- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
- Los documentos que contengan información sensible no deben ser reutilizados y destruirse de acuerdo con los parámetros y normatividad vigente del Archivo General.

21. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

Gestión TIC's es el encargado de la operación y administración de los recursos tecnológicos que apoyan y soportan los procesos de la Corporación, al igual que propende por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información, asegurando que los cambios efectuados sobre los recursos tecnológicos, sean los adecuados y autorizados de acuerdo a los informes de seguridad de las casas fabricantes. Así mismo, provee la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, proyectando el crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Corporación.

21.1 POLÍTICA DE PROTECCIÓN FRENTE A CIBERATAQUES

La Corporación de la Industria Aeronáutica Colombiana - 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:

- Gestión TIC's 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.
- Los sistemas operativos y software, especialmente el del antivirus, antimalware, antispam, antispyware, entre otras, deben contar con las últimas actualizaciones y parches de seguridad.
- Los usuarios no pueden realizar cambios en la configuración del software de antivirus, antimalware, antispam y antispyware, únicamente pueden realizar tareas de escaneo de virus.
- Los equipos de cómputo y servidores de CIAC, deben contar con un antivirus actualizado.
- 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.
- 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.

- 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.

21.2 POLÍTICA DE COPIAS DE RESPALDO Y RECUPERACIÓN

Gestión TIC's adopta las medidas necesarias para garantizar la disponibilidad y la integridad de las copias de respaldo mediante pruebas regulares de restauración, asegurando que los datos puedan ser recuperados de manera efectiva en caso de una eventualidad y que las copias de respaldo cumplan con los estándares de calidad establecidos.

21.2.1 Copias de Respaldo

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

- CIAC proporciona como herramienta para llevar a cabo el proceso de copia de respaldo o backup 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 respaldo o backup.
- Cada usuario es responsable de realizar la copia de respaldo o backup de los archivos importantes para evitar pérdidas de información que puedan llegar a ser vitales para el funcionamiento de la Corporación.
- Se recomienda hacer mínimo una vez a la semana la copia de respaldo o backup o con la periodicidad que considere necesarias de acuerdo con la criticidad de la información para mitigar el riesgo de pérdida de información.
- En caso de requerir apoyo para realizar la copia de respaldo o backup, se debe solicitar a Gestión TIC's mediante Ticket en la herramienta destinada como mesa de ayuda.
- El coordinador, jefe o director de área, oficina o grupo puede solicitar mediante Ticket en la herramienta destinada como mesa de ayuda, realizar una copia de respaldo de la información que manejan sus colaboradores.
- En caso de retiro de personal, el coordinador, jefe o director de área, oficina o grupo es el responsable de verificar y recibir la copia de seguridad de la información digital del usuario, tanto del equipo de cómputo, OneDrive y correo electrónico.

- Antes de terminar la vinculación laboral con un colaborador, Gestión de Talento Humano, el coordinador, jefe o director de área, oficina o grupo, debe informar a Gestión TIC's para tomar las medidas de seguridad necesarias para evitar fuga o pérdida de información digital.
- 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 respaldo o backup 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.
- Las copias de respaldo deben almacenarse tanto localmente como en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental y de control de acceso físico.
- Revisar y/o actualizar periódicamente las configuraciones de los servidores para la correcta ejecución de las copias de respaldo.
- 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 semanalmente el informe de la copia de respaldo 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 respaldo 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)

21.2.2 Restauración

- Realizar pruebas de restauración sobre las copias de respaldo por lo menos una (1) vez por semestre, esta frecuencia puede ajustarse según las necesidades operativas y la criticidad de los datos respaldados.
- Seleccionar aleatoriamente copias de respaldo para las pruebas de restauración. Estas pruebas verificarán que los datos puedan ser recuperados de manera efectiva y que los procedimientos de restauración sean adecuados.
- Durante las pruebas de restauración, se verificará tanto la integridad como la disponibilidad de los datos; cualquier discrepancia o problema identificado será registrado y abordado de manera inmediata.
- Destinar un servidor específico para llevar a cabo las pruebas de restauración. Este servidor será utilizado exclusivamente con fines de prueba y no afectará los sistemas de producción.
- Después de cada prueba de restauración, debe quedar el registro detallado con los siguientes datos:

  - Nombre del servidor restaurado
  - Fecha de la copia recuperada
  - Informe paso a paso de la restauración, documentando todas las etapas del proceso de recuperación.
  - Informar cualquier problema o anomalía encontrada durante la prueba y su posible acción de mejora.
- Los resultados de las pruebas de restauración deben ser revisados y evaluados de manera regular. Cualquier patrón de problemas identificados llevará a investigaciones y mejoras en los procedimientos de respaldo.
- Gestión TIC's es el responsable de coordinar y ejecutar las pruebas de restauración, al igual que documentar los resultados.
- 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.

21.3 POLÍTICA DE ONEDRIVE

Se establecen las siguientes directrices para garantizar la integridad y la disponibilidad de los datos críticos almacenados en los equipos de la Corporación mediante la implementación de una solución de sincronización y respaldo utilizando Microsoft OneDrive para asegurar que los archivos en las carpetas de Escritorio, Documentos, Imágenes y las carpetas que contengan información de valor para los usuarios se respalden automáticamente en la nube:

- En cada equipo de la Corporación, se llevará a cabo la configuración de Microsoft OneDrive para sincronizar automáticamente las carpetas de Escritorio, Documentos e Imágenes. Esto se realizará utilizando la última versión estable de la aplicación OneDrive proporcionada por Microsoft.
- Cuando se realice una reinstalación del sistema operativo en un equipo de cómputo, el personal de Gestión TICS se encargará de la configuración de OneDrive en el perfil del usuario, esto involucra la sincronización de las carpetas esenciales, como Escritorio, Documentos e Imágenes.
- Para respaldar información diferente a las carpetas de Escritorio, Documentos e Imágenes, Gestión TIC's presta el soporte mediante Ticket en la herramienta destinada como mesa de ayuda.
- La sincronización de archivos con OneDrive se realiza de manera continua y automática. Los archivos en las carpetas designadas se actualizarán en tiempo real y reflejarán los cambios en la nube y en los equipos.
- OneDrive mantendrá copias incrementales y versionadas de los archivos en la nube de manera segura y accesible, esto permitirá la recuperación de versiones

anteriores en caso de errores o cambios no deseados, adicionando una capa de protección contra pérdida de datos debido a fallos en los equipos.

- Se verificará regularmente el estado de la sincronización de OneDrive en los equipos, cualquier problema o novedad será tratado de manera inmediata para garantizar la integridad de los datos.
- En caso de que se presente alguna novedad en la sincronización de los archivos se debe solicitar el soporte por medio de Ticket en la herramienta destinada como mesa de ayuda.
- Se llevarán a cabo pruebas regulares de recuperación utilizando los datos sincronizados en OneDrive. En estas pruebas se verificará la efectividad de los procedimientos de recuperación y la disponibilidad de los datos respaldados.
- Los usuarios son los responsables de verificar por lo menos una (1) vez a la semana que las copias en OneDrive se estén ejecutando de manera correcta.
- Gestión TIC's es el responsable de implementar, configurar y supervisar la solución de OneDrive en todos los equipos de la Corporación.
- Es responsabilidad de cada usuario asignar los niveles de acceso (editar, ver o revisar) a las carpetas que comparte por OneDrive.
- El equipo de Gestión de TIC se encargará de proporcionar capacitación y soporte integral a los usuarios sobre el uso correcto y eficiente de OneDrive, asegurando que comprendan cómo sincronizar, acceder, gestionar y dar acceso a sus archivos de manera adecuada.

21.4 POLÍTICA DE SOFTWARE OPERACIONAL

Gestión TIC's controla la instalación de software asegurando la integridad y funcionalidad de los sistemas de información, cerciorándose que cumplan con los requerimientos legales y de licenciamiento aplicables.

Se establecen las siguientes directrices para la instalación de software en sistemas operativos:

- Gestión TIC's debe cerciorarse que el software operativo instalado en la plataforma tecnológica cuente con el respetivo soporte de los proveedores y fabricantes si se requiere.
- Gestión TIC's debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo en caso de ser requerido. Así mismo, monitorear tales actualizaciones, estar pendiente mientras esté conectado el proveedor y grabar la sesión como evidencia de los ajustes realizados.

- Todo software que se instale en los activos de información debe cumplir con los requerimientos legales y de licenciamiento aplicables, es decir, deben tener derechos de autor, licencia de uso o de libre distribución y uso.
- Validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- Las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Corporación, está sujeto al licenciamiento que se haya adquirido y en todo caso los equipos de cómputo o servidores deben tener el respectivo licenciamiento.
- El control de las actualizaciones se realiza a través de la herramienta tecnológica utilizada para el parcheo y actualizaciones que emitan las casas fabricantes de este software.

21.5 POLÍTICA DE GESTIÓN DE VULNERABILIDADES TÉCNICAS

Gestión TIC's revisa las vulnerabilidades técnicas sobre los recursos y servicios tecnológicos mediante pruebas, con el fin de identificar, evaluar y mitigar posibles debilidades de los sistemas.

Se establecen las siguientes directrices para la gestión de vulnerabilidades:

- Se realizarán evaluaciones periódicas de vulnerabilidades utilizando herramientas y técnicas de escaneo, pruebas de penetración y revisión de boletines de seguridad.
- Analizar las vulnerabilidades reportadas por el proveedor de seguridad perimetral y antivirus.
- Generar y ejecutar planes de acción para la mitigación de las vulnerabilidades detectadas y cerrar las posibles brechas de seguridad.
- Realizar pruebas semestrales de vulnerabilidades con el fin de identificar y mitigar riesgos.
- Tomar las medidas adecuadas para reducir los riesgos resultantes de las pruebas de vulnerabilidad.
- Capacitar y concientizar a los usuarios

22. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

Gestión TIC's propende por el aseguramiento y disponibilidad de las redes de datos y el control del tráfico, mediante mecanismos de seguridad que protejan la integridad y confidencialidad de la información que se transporte a través de estas redes, además de

establecer acuerdos para el intercambio seguro de información dentro de la Corporación y con cualquier entidad externa.

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

- CIAC dispondrá de los recursos necesarios para la correcta operación de la infraestructura tecnológica de red.
- Las redes inalámbricas de la Corporación deben contar con métodos de autenticación que eviten accesos no autorizados y/o la utilización de dispositivos personales.
- 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.

23. POLÍTICA DE SEGURIDAD ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Gestión TIC’s es la única dependencia con la capacidad de adquirir, desarrollar e implementar o avalar la adquisición, desarrollo y mantenimiento de los sistemas de información y comunicación, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que opera en la Corporación.

Se establecen las siguientes directrices para la adquisición, desarrollo y mantenimiento de sistemas de información:

- Cualquier software o aplicativo que opere en la CIAC debe contar con la autorización de Gestión TIC’s, debe reportarse y entregarse a esta dependencia cumpliendo los lineamientos técnicos y presupuestales, con el fin de proteger la información, brindar

el soporte y los demás procesos técnicos requeridos que permitan su recuperación en caso de algún incidente o siniestro.

- Contemplar todo lo concerniente a seguridad digital, ciberseguridad y accesibilidad web para todos los sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde el diseño y levantamiento de requerimientos, hasta las pruebas de vulnerabilidades una vez el software se encuentre en producción, teniendo en cuenta los riesgos asociados a cada sistema de información.
- Los sistemas de información adquiridos o desarrollados por terceros deben estar acordes con la tecnología vigente y para lo que se contrató.
- Los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del Software y los derechos de propiedad intelectual según lo contratado.
- Los proveedores de sistemas de información deben suministrar la información de requerimientos técnicos necesarios para el óptimo funcionamiento del software.
- Deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla el tiempo establecido.
- Suministrar opciones de desconexión o cierre de sesión de los aplicativos (LOGOUT) que permitan terminar completamente con la sesión o conexión asociada.
- No divulgar información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, se deben implementar mensajes de error genéricos que induzcan a una pronta solución.
- Todo software debe contar con el nivel de soporte requerido y la capacitación adecuada para el uso de la Corporación y Gestión TIC's.
- Realizar pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse de acuerdo con las funciones y a los requerimientos para los cuales se está probando, verificado siempre por el dueño del proceso.
- Los colaboradores son los responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en la Corporación, por lo tanto, deben alimentar los datos que son editables en forma íntegra y verás.
- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios.

24. CUMPLIMIENTO

24.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

La Corporación de la Industria Aeronáutica Colombiana - 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.

24.1.1 Derechos de Autor y Propiedad Intelectual

La Corporación de la Industria Aeronáutica Colombiana - CIAC mediante Gestión TIC's propende 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.
- Adquirir software mediante fuentes conocidas y confiables.
- El software utilizado debe contar con las licencias de uso requeridas, certificando así su autenticidad y legalidad.
- Implementar controles para que no se excedan el número máximo de usuarios permitidos de las licencias.
- Revisar que solo esté instalado software autorizado y productos con licencia.

24.1.2 Protección de Datos Personales

La Corporación de la Industria Aeronáutica Colombiana - 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 tratamiento de datos personales contemplada en la **Resolución N° 013 del 25 de enero de 2023** *"Por medio de la cual se adopta la política para el tratamiento de datos personales, se designa y establecen las competencias del oficial de datos personales de la Corporación de la Industria Aeronáutica Colombiana S.A."*

24.2 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 la

materialización de un riesgo, o por nuevas disposiciones legales que apliquen para asegurar su eficiencia y efectividad. 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.

24.3 SANCIONES

Las políticas establecidas en el presente manual instituyen y afianzan la cultura de seguridad de la información entre los colaboradores, 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.