MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La gestión de seguridad de la información implica la organización y coordinación de todos los esfuerzos encaminados al aseguramiento del entorno informático del Instituto, para lo cual es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por los funcionarios y terceros del Instituto.

La Política de Seguridad de la Información es la declaración general que representa la posición de la Dirección del ICFE con respecto a la protección de los activos de información.

El presente documento se encuentra estructurado con una Política General de Seguridad de la Información y Políticas Específicas que soportan el Sistema de Gestión de Seguridad de la Información, las cuales deben ser conocidas y aceptadas por todos los usuarios de la infraestructura tecnológica y la información del Instituto.

2. JUSTIFICACIÓN

La Resolución No 065 del 24 de mayo de 2016, del ICFE, por medio de la cual se adopta la Directiva No 2014-18 del 19 de junio de 2014 “Políticas de Seguridad de la Información para el Sector Defensa”, establece la elaboración del Manual de Seguridad de la Información para el Instituto.

3. OBJETIVO

Dar a conocer a todos los funcionarios y terceros del Instituto, las políticas y estándares que se deben cumplir para proteger y/o preservar los activos de información.

4. ALCANCE

Las Políticas definidas en el presente manual aplican a toda la entidad, empleados públicos, trabajadores oficiales, personal militar en comisión, contratistas y pasantes del ICFE, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y Seguridad de la Información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección del Instituto.

5. DEFINICIONES

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su recurrencia. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.9]*

- **Actividad:** Conjunto de una o más tareas con un resultado específico. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.1]*

- **Actividad priorizada:** Actividad a la cual se le da urgencia con el fin de evitar impactos indeseables para el negocio durante una interrupción. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.25]*

- **Acuerdo de confidencialidad:** Un acuerdo de confidencialidad es un documento que se firma entre partes, en el cual se comprometen a no divulgar ni compartir información que manejan por motivos de trabajo, o de participación en algún proyecto u emprendimiento. Es decir, se comprometen a mantener la confidencialidad de la información a la que tienen acceso. *[ConceptosJuridicos.com URL: https://www.conceptosjuridicos.com/acuerdo-de-confidencialidad/]*

- **Acuerdo de Nivel de Servicio (ANS o SLA por sus siglas en inglés):** Acuerdo documentado entre un prestador de servicios y un cliente, el cual identifica los servicios y los objetivos del servicio. *[Norma ISO 20000:2012, Capitulo 3, Términos y definiciones, numeral 3.3]*

- **Alta dirección**: Persona o grupo de personas que dirigen y controlan una organización en su más alto nivel. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.31]*

- **Análisis de impacto al negocio (BIA, por sus siglas en inglés):** Proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo, en la organización. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.5]*

- **Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.2]*

- **Control**: Medida que modifica un riesgo. *[Norma ISO 27000:2017, Capitulo 2, Términos y definiciones, numeral 2.16]*

- **Competencia:** Habilidad de aplicar los conocimientos y las habilidades para lograr los resultados deseados. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.6]*

- **Conformidad:** Cumplimiento de un requisito*. [Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.7]*

- **Continuidad del negocio:** Capacidad de una organización de continuar la oferta de productos y servicios dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción*. [Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.3]*

- **Desempeño:** Resultado medible. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.23]*

- **Disparador:** Evento que hace que el sistema inicie una respuesta. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.15]*

- **Eficacia:** Grado en el cual se realizan las actividades planeadas y se logran los resultados esperados. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.12*

- **Equipos de continuidad del negocio:** Grupo de personas responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución de los planes de continuidad de la organización. *[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]*

- **Estimación del riesgo.** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. *[Norma ISO 27005:2009, Capitulo 3, Términos y definiciones, numeral 3.5]*

- **Evitar el riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. *[Norma ISO 27005:2009, Capitulo 3, Términos y definiciones, numeral 3.3]*

- **Fuente de riesgo:** Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo. *[Norma ISO 31000:2018, Capitulo 3, Términos y definiciones, numeral 3.4]*

- **Gestión de continuidad del negocio (BCM, por sus siglas en inglés)***:* Proceso general que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que, en caso de materializarse, y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.2]*

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar la organización con relación al riesgo*. [Norma ISO 31000:2018, Capitulo 3, Términos y definiciones, numeral 3.2]*

- **Impacto:** Resultado de una interrupción que afecta los objetivos. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.13]*

- **Incidente:** Evento que puede ser, o podría conducir a una interrupción *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.14]*

- **Información documentada:** Información que una organización tiene que controlar y mantener, y el medio que la contiene. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.11]*

- **Interrupción:** Incidente, bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.10]*

- **Malware:** Abreviatura de software malicioso. Diseñado para infiltrarse, dañar u obtener información de un sistema informático sin el consentimiento del propietario ***Nota***: El malware se considera comúnmente para incluir virus informáticos, gusanos, troyanos, spyware y adware. El spyware se utiliza generalmente con fines de marketing y, como tal, no es malicioso, aunque generalmente no es deseado. Sin embargo, el spyware se puede utilizar para recopilar información para el robo de identidad u otros fines claramente ilícitos. [ISACA:2015 - Glosario de términos – URL: https://www.isaca.org/resources/glossary]

- **MAO – Maximum acceptable outage –** Ver MTPD

- **Medición:** Proceso para determinar un valor. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.17]*

- **Mejoramiento continuo:** Actividad recurrente para mejorar el desempeño. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.8]*

- **Modo de falla:** Manera por la cual una falla es observada. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.9]*

- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.18]*

- **MTPD – Maximum tolerable period of disruption:** Tiempo que tomaría para que los impactos adversos, que pueden surgir como resultado de no proporcionar un producto/servicio o realizar una actividad, se vuelvan inaceptables *[Norma ISO 22300:2021, Capitulo 3, Términos y definiciones, numeral 3.1.151]*

- **Nivel de decisión estratégico:** El nivel de decisión estratégico relacionado con la continuidad del negocio se refiere a las decisiones que se toman a nivel ejecutivo para garantizar la supervivencia y la resiliencia de una organización frente a posibles interrupciones o desastres. *[Bajgoric, N., & Hadziahmetovic, N. (2019). Strategic Decision Making in the Field of Business Continuity Management: Conceptual Framework. Journal of Contemporary Management Issues, 24(1), 83-103.]*

- **Nivel de decisión operativo:** El nivel de decisión operativo relacionado con la continuidad del negocio se refiere a las decisiones que se toman a nivel de la línea de frente o de la ejecución diaria para garantizar la implementación efectiva de los planes y procedimientos establecidos a niveles estratégicos y tácticos. *[Elliot, S., Swartz, E., & Herbane, B. (2010). Business continuity management: A crisis management approach. In The Handbook of Crisis Communication (pp. 298-320). Wiley-Blackwell.]*

- **Nivel de criticidad***:* Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra. *[Guía Nro 10 para la preparación de las TIC para la continuidad del negocio, Capitulo 5, Glosario]*

- **Nivel de decisión táctico:** El nivel de decisión táctico relacionado con la continuidad del negocio implica tomar decisiones operativas a corto y mediano plazo para implementar los planes y estrategias establecidos a nivel estratégico. Estas decisiones se centran en la gestión de recursos y actividades específicas para mantener la continuidad de las operaciones durante situaciones de emergencia o crisis*. [Bajgoric, N., & Hadziahmetovic, N. (2019). Strategic Decision Making in the Field of Business Continuity Management: Conceptual Framework. Journal of Contemporary Management Issues, 24(1), 83-103]*

- **No conformidad:** Incumplimiento de un requisito. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.19]*

- **Objetivo:** Resultado a lograr. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.20]*

- **Objetivo mínimo de continuidad del negocio (Minimum Business Continuity Objective – MBCO, por sus siglas en inglés):** Mínimo nivel de servicios y/o productos que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.11]*
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridad y relaciones para lograr sus objetivos. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.21]*

- **Parte interesada - término preferido- / Accionista (stakeholder) - término admitido:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. Ejemplo: Clientes, propietarios, personal de una organización, proveedores, banca, legisladores, sindicatos, socios o sociedad que pueden incluir competidores o grupos de presión con intereses opuestos. Se consideran partes interesadas las comunidades impactadas y las poblaciones locales se consideran partes interesadas. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.15]*

- **Plan de continuidad del negocio (BCP, por sus siglas en inglés)***:* Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.3]*
- **Plan de Recuperación ante Desastres de TIC (DRP):** Plan claramente definido y documentado el cual permite recuperar las capacidades de la tecnología y las telecomunicaciones cuando se presenta una interrupción. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.14]*

- **Política:** Propósitos y dirección de una organización, como expresa formalmente la alta dirección. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.24]*

- **Probabilidad**: Posibilidad de que algo ocurra. *[Norma ISO 31000:2018, Capitulo 3, Términos y definiciones, numeral 3.7]*

- **Programas utilitarios:** Los programas utilitarios son programas que brindan una "utilidad" específica y no están diseñados para un tipo de usuario particular. Ejemplo, procesadores de texto, planillas de cálculo, videojuegos, navegadores para la web, etc.

- **Plan de continuidad del negocio:** Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.4]*

- **Preparación de las TIC para la continuidad de negocio (ICT Readiness for Business Continuity - IRBC, por sus siglas en inglés):** Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción, así como la recuperación de sus servicios de TIC. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.10]*

- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan las cuales transforman entradas en salidas. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.26]*

- **Productos y servicios:** Salida o resultado que provee una organización a las partes interesadas. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.27]*

- **Punto objetivo de recuperación (RPO, Recovery Point Objetive, por sus siglas en inglés):** Punto en el tiempo en el cual los datos deberían ser recuperados después de que una interrupción ocurra. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.12]*

- **Recursos:** Todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (bien sea electrónica o no) que una organización posee y que tienen que tener disponibilidad para usarse cuando sea necesario, con el fin de operar y lograr su objetivo*. [Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.29]*

- **Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. *[Norma ISO 27005:2009, Capitulo 3, Términos y definiciones, numeral 3.7]*

- **Registro vital:** Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.16]*

- **Requisito:** Necesidad o expectativa que se indica, generalmente implícita u obligatoria.

[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.28]

- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. *[Norma ISO 27005:2009, Capitulo 3, Términos y definiciones, numeral 3.8]*

- **Resiliencia***:* Habilidad para una organización para resistir al ser afectada por una interrupción. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.14]*

- **Riesgo**: Efecto de la incertidumbre en los objetivos. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.30]*

- **Riesgo residual:** Riesgo remanente después del tratamiento del riesgo. *[Norma ISO 27000:2017, Capitulo 2, Términos y definiciones, numeral 2.64]*

- **Servicios tecnológicos:** Conjunto de actividades basadas en la tecnología que buscan responder a las necesidades de los usuarios. Dentro de los servicios tecnológicos se encuentran, entre otros: los servicios tecnológicos de bases de datos, los servicios tecnológicos de comunicaciones LAN / WAN e internet, los servicios tecnológicos de seguridad, los servicios tecnológicos de almacenamiento y virtualización, los servicios tecnológicos de la nube (web, email y redes sociales).

- **Sistema de gestión:** Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr esos objetivos. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.16]*

- **Sitio alterno:** Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevare a cabo utilizando las instalaciones normales después de que se ha producido una interrupción. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.1]*

- **Subcontratar:** Realizar un acuerdo donde una organización externa realiza parte de una función o proceso de la organización. Nota: Una organización externa esta por fuera del alcance del sistema de gestión, aunque la función o proceso subcontratado esté dentro del alcance. *[Norma ISO 22301:2019, Capitulo 3, Términos y definiciones, numeral 3.22]*

- **Tercero / Proveedor**: Persona natural o jurídica con quien se vincula la Entidad para apoyar la ejecución de sus macroprocesos estratégicos, misionales, apoyo y evaluación en aras de cumplir los objetivos del negocio.

- **Tiempo objetivo de recuperación (RTO, Recovery Time Objective, por sus siglas en inglés):** Periodo de tiempo en el cual los mínimos niveles de servicios y/o productos y los sistemas, aplicaciones o funciones que los soportan deben ser recuperados después de que una interrupción ocurra. *[ISO/IEC 27031:2016, Capitulo 3, Términos y definiciones, numeral 3.13]*

- **Transferencia del riesgo.** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. *[Norma ISO 27005:2009, Capitulo 3, Términos y definiciones, numeral 3.9]2000*

- **WRT – Working Recovery Time:** Es la cantidad máxima tolerable de tiempo que tiene un equipo de recuperación ante desastres para verificar que los sistemas y la protección de datos estén en línea y operativos. WRT es la fase posterior a la restauración de los datos y las operaciones de misión crítica, cuando la organización debe concentrarse en volver a la normalidad.

6. MARCO LEGAL

- Constitución Política de Colombia 1991.
- Ley 80 de 1993 “Estatuto General de contratación de la administración Pública”.
- Ley 87 de 1993 “Control interno en los organismos del Estado”.
- Ley 527 de 1999 “Comercio Electrónico”.
- Ley 594 del 2000 “Ley General de Archivo”.
- Ley 599 del 2000 “Código Penal Colombiano”.
- Ley 603 del 2000 “Control de legalidad del Software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información”.
- Ley 1273 de 2009 “Protección de la Información y de los datos”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia.
- Norma Técnica Colombiana NTC-ISO/IEC 27001-2022 Seguridad de la información, ciberseguridad y protección de la privacidad
- Directiva No 2014-18 “POLIITCAS DE SEGURIDAD DE LA INFORMACION PARA EL SECTOR DEFENSA”.

7. REVISIÓN DE LAS POLÍTICAS

Las Políticas de Seguridad de la Información del presente manual serán revisadas anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la Política. Con el fin de asegurar que se encuentren ajustadas a los requerimientos del Instituto.

8. COMPROMISO DE LA DIRECCIÓN

La Dirección General del ICFE aprueba este Manual de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Dirección del Instituto demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las Políticas de Seguridad de la Información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

9. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los lineamientos de seguridad de la información, ciberseguridad y protección de la privacidad presentados a continuación cuentan con su respectiva justificación de su definición y la descripción de los elementos que se consideran generalmente en el Sistema de Gestión de seguridad de la información (SGSI).

10. CONTROLES ORGANIZACIONALES

10.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El ICFE se compromete con el cumplimiento de los lineamientos del Sector Defensa, preservando los atributos de confidencialidad, integridad y disponibilidad de la información, promoviendo una cultura de seguridad y administrando los riesgos de los activos de información, mediante el establecimiento, implementación, mantenimiento y mejoramiento continuo de las políticas de seguridad de la información, contribuyendo con la misión, visión y objetivos estratégicos del Instituto.

OBJETIVOS

- Proteger los recursos de información y tecnología utilizados para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.
- Implementar un Sistema de Gestión de Seguridad de la Información, orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información en el Instituto.
- Promover, mejorar y mantener un nivel de cultura en seguridad de la información, así como lograr la concientización de todos los funcionarios y terceros que interactúan con el Instituto, para minimizar la ocurrencia de incidentes de seguridad de la información.
- Identificar, caracterizar y valorar los activos de información para determinar su criticidad y establecer medidas de protección sobre los mismos.
- Mitigar el impacto y probabilidad de ocurrencia de los riesgos de ciberseguridad y emergentes asegurando la implementación de controles y monitoreando su eficacia de forma continua.

  Gestionar y dar respuesta oportuna de los incidentes de seguridad de la información que puedan presentarse asegurando su contención, erradicación y respuesta.

10.2. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

10.2.1. Oficial de Seguridad de la Información

a) Gestionar y mantener la gestión de seguridad de la información, asegurando que se cuente con todas las medidas de protección requeridas para los activos de información y la plataforma tecnológica de ICFE a través de procesos de monitoreo y mejora continua.
b) Asegurar la Identificación, caracterización y valoración los activos de información por los propietarios, para determinar su criticidad y establecer medidas de protección sobre los mismos.
c) Mitigar el impacto y probabilidad de ocurrencia de los riesgos de ciberseguridad asegurando la implementación de controles y monitoreando su eficacia de forma continua.
d) Gestionar los incidentes de seguridad de la información que puedan presentarse asegurando se ejecuten etapas de contención, erradicación y respuesta de forma oportuna.
e) Fortalecer la cultura y conciencia de seguridad en los usuarios, terceros y clientes que tienen acceso a los activos de información en uso por la compañía.
f) Reportar anualmente al Comité designado para el monitoreo y control del SGSI sobre el desempeño en la gestión de Seguridad de la Información adicionalmente generar propuestas de mejora en materia de ciberseguridad y comportamiento de los incidentes de seguridad de la información que afectaron la compañía incluyendo el panorama de amenazas.
g) Verificar periódicamente el cumplimiento de los requisitos de seguridad en los contratos y servicios provistos con proveedores o terceros críticos.
h) Establecer lineamientos y verificar la implementación de mecanismos para la adecuada autenticación, segregación de las funciones de los usuarios que acceden a la red de ICFE.

10.2.2. Ingeniero de Seguridad de la Información

a) Definir y establecer las políticas de seguridad de la información, alineadas con las emitidas por el Ministerio de Defensa Nacional.
b) Coordinar la implementación de las políticas de Seguridad de la Información con los diferentes procesos del Instituto.
c) Reportar a la Jefatura de Informática el estado de la Seguridad de la Información del Instituto.
d) Definir e implementar la estrategia de divulgación y concientización de Seguridad de la Información para todos los funcionarios y terceros que tengan acceso a los activos de información del Instituto.
e) Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten la labor de seguridad de la información.

f) Coordinar y ejercer control en el cumplimiento de las Políticas de Seguridad de la Información.

10.2.3. Líderes de cada uno de los procesos de la compañía

a) Participar en las auditorías y gestionar los resultados en conjunto con el responsable de administrar la gestión de seguridad de la información.
b) Participar de la revisión en conjunto con el Oficial de Seguridad de la información designado para el monitoreo y control del SGSI, demostrando así su compromiso con la gestión de seguridad de la información.
c) Velar porque su equipo y todas las actividades que realizan cumplan con las políticas de Gestión de Seguridad de la Información, y apoyar la concientización y socialización de estas.
d) Identificar y gestionar oportunamente los incidentes de seguridad de su proceso.
e) Identificar y gestionar los riesgos que se encuentran en su proceso y velar por la implementación de los planes de tratamientos para su mitigación.
f) Garantizar que los activos de información de su proceso sean identificados, clasificados y protegidos adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso.
g) Gestionar la mejora continua de su proceso, así como las acciones correctivas y de mejora asociadas a la gestión de seguridad de la información.
h) Definir y controlar los niveles de acceso a la información del proceso teniendo en cuenta la clasificación y los usuarios que la necesiten.
i) Garantizar que la documentación del proceso sea vigente frente a las actividades realizadas.
j) Cumplir con la política de tratamiento de los datos personales y los estándares definidos para la correcta recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se traten en ICFE.

10.2.4. Funcionarios y usuarios de los sistemas de información

a) Todos los funcionarios del Instituto, empleados públicos, trabajadores oficiales, personal militar en comisión, contratistas y pasantes, son responsables por el cumplimiento de las Políticas de Seguridad de la Información. Adicionalmente están comprometidos a reportar por escrito al correo del Ingeniero de Seguridad de la Información cualquier evento o incidente de seguridad del que tenga conocimiento.
b) Participar en los procesos de auditoría, suministrando información cuando sea requerido.
c) Identificar los riesgos que se encuentran en sus actividades y apoyar en la definición de planes de tratamientos para mitigarlos.
d) Participar activamente en la mejora continua de la seguridad de la información de ICFE.
e) Cumplir los acuerdos de confidencialidad establecidos con la compañía.
f) Responder adecuadamente por los activos asignados y los de la compañía.

Cumplir con la política de tratamiento de los datos personales y los estándares definidos para la correcta recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales.

10.2.5. Los roles y responsabilidades de proveedores o terceros serán definidos a través de los contratos u orden de compra o servicio, así como a través de las cláusulas relacionadas en el acuerdo de confidencialidad en donde se comprometen como mínimo a:

a) Abstenerse de divulgar en cualquier forma o de utilizar en provecho propio o ajeno, la información de carácter confidencial o restringida que se haya conocido en ejercicio de sus funciones.
b) Los proveedores que tengan acceso a información confidencial deben protegerla y resguardarla.
c) Firmar un acuerdo de confidencialidad en donde queden especificadas las responsabilidades para el intercambio de la información entre las partes; el acuerdo se firma antes de permitir el acceso a la información de ICFE.
d) Cumplir con las disposiciones legales aplicables, así como aquellas normas internas adoptadas en materia de seguridad de la información.
e) Conocer y aplicar la Política de seguridad de la información al interior de su compañía.
f) Implementar buenas prácticas y estándares internacionales de ciberseguridad en la configuración de los sistemas de información.
g) Responder adecuadamente por los activos asignados y los de la compañía.
h) Cumplir con la política de tratamiento de los datos personales y los estándares definidos para la correcta recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales.
i) Asegurar la protección de la confidencialidad, integridad y disponibilidad de los activos de información proporcionados como parte del objeto del contrato u orden de compra.
j) Notificar los incidentes de seguridad de forma inmediata, una vez se tenga conocimiento de estos, gestionarlos y reportar el plan de tratamiento correspondiente.
k) Informar oportunamente cualquier cambio o modificación en el servicio que pueda afectar la información.

10.2.6. Administradores de los Sistemas de Información

Los administradores de los diferentes sistemas deben en forma activa implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información, de acuerdo con las políticas de seguridad de la información del ICFE.

10.2.7. Oficina de Control Interno

Realizar auditorías a los procesos del Sistema de Gestión de Seguridad de la Información, una vez implementado, como mínimo una vez al año.

10.2.8. Oficina de Contratos

Esta dependencia tiene dentro de sus funciones realizar la revisión de requisitos para proceder a la posesión como servidor público. Como parte de la función de selección se debe realizar una verificación de los antecedentes y referencias de los candidatos, garantizar que los funcionarios firmen el acuerdo de confidencialidad.

10.2.9. Oficina Asesora Jurídica

Esta oficina es la responsable de garantizar que se incluyan las cláusulas de confidencialidad de la información dentro de los contratos de los contratistas.

10.3. SEGREGACIÓN DE FUNCIONES

Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos, para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información debe ser revisada periódicamente por la oficina de Informática, con el fin de mantener actualizada dicha información acorde con la realidad del ICFE.

Se debe implementar mecanismos para segregar las funciones en las áreas de negocio que puedan presentar cualquier tipo de conflicto de interés, asegurando así la reducción de riesgo de fraude, error y/o elusión de los controles de seguridad de la información.

Cuando no sea posible segregar las funciones debido a limitaciones en la cantidad de personal que ejecuta la actividad, se debe implementar controles compensatorios relacionados con seguimientos, auditorías o supervisiones continuas.

10.4. CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL

El Oficial de Seguridad de la Información debe definir y establecer el listado de contacto con las autoridades en donde se contemple cuando, por quien y como se debe informar oportunamente los incidentes identificados. Así mismo ICFE debe participar de grupos de interés especial, foros especializados en seguridad y asociaciones profesionales para mantenerse actualizado y preparado respecto a los cambios normativos aplicables, los cambios en el entorno, mejores prácticas en seguridad y nuevas tecnologías.

A continuación, se relaciona el listado de principales contactos con algunas autoridades y grupos de interés:

- Centro Cibernético de la Policía Nacional / https://caivirtual.policia.gov.co.

- colCERT / Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia / contacto@colcert.gov.co .
- Csirt Gobierno de Colombia / csirtgob@mintic.gov.co
- Superintendencia de industria y comercio “incidentes de seguridad sobre datos personales” / https://rnbd.sic.gov.co/sisi/login.
- Bomberos / https://www.bomberosbogota.gov.co/transparencia/atencion-ciudadano/estaciones / Línea de emergencia 123.

11.

10.5. INTELIGENCIA DE AMENAZAS

ICFE hace recolección y análisis de inteligencia de amenazas buscando generar información sobre amenazas y de esta manera facilitar las acciones para evitar y mitigar los riesgos que causen daño a la compañía y reducir su impacto.

10.6. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información debe integrarse en la gestión de proyectos para garantizar que los riesgos de seguridad de la información se aborden como parte de la gestión de este.
Esto se aplicará a los proyectos de mayor complejidad, tamaño, duración, disciplina o área de aplicación.

Se debe asegurar:

- La definición de requisitos de seguridad considerados desde las primeras etapas del proyecto y periódicamente durante su ejecución, por ejemplo: requisitos de seguridad en aplicaciones y desarrollo seguro, comunicación interna y externa, requisitos de continuidad o propiedad intelectual.
- La identificación y tratamiento de riesgos de seguridad de la información en todo el ciclo de vida del proyecto y la efectividad de estas.
- Los roles y responsabilidad de seguridad de la información que participarán en la gestión de proyectos.
- Las necesidades de protección sobre la información y los activos involucrados.
- El cumplimiento del entorno legal, estatutario, reglamentario y contractual que aplica a la compañía.

10.7. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Los activos de información del ICFE, serán identificados, clasificados y valorados para establecer los mecanismos de protección necesarios, de acuerdo con el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION; así mismo tendrán un propietario asociado quien es el responsable de definir quienes tienen acceso y que pueden hacer con la información.

Todos los servidores públicos y terceros que utilicen los recursos TIC deben seguir las políticas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, establecidos por la Entidad.

Uso aceptable de la información y otros activos asociados:

- El uso de los activos de la compañía debe estar autorizado y ser adecuado para el desempeño de las funciones laborales del usuario.
- Los usuarios deben asegurarse de que la información y los activos de la ICFE estén protegidos y sean utilizados de manera responsable.
- El acceso y uso de la información de los activos de la ICFE deben ser limitados a los usuarios autorizados.
- Los usuarios no deben compartir información o activos de la ICFE con terceros sin la debida autorización.

10.7.1. Devolución de activos

Como parte del ICFE-P-140-F-03 ENTREGA PUESTO DE TRABAJO Y TRANSFERENCIA DE CONOCIMIENTO, es esencial proteger los activos de la compañía. El personal de ICFE, los proveedores y otras partes interesadas deben devolver todos los activos de la compañía que posean. Es necesario identificar y documentar claramente todos los activos e información que deben ser devueltos al concluir la relación laboral. En caso de que no sea posible la devolución de los activos, se implementarán controles compensatorios, tales como la gestión de derechos de acceso o el uso de criptografía.

10.7.2. Clasificación de la información

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere el ICFE como, por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información transmitida vía oral o por cualquier otro medio de comunicación.

EL ICFE estableció en el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION los criterios para realizar la valoración de los mismos respecto a su nivel de confidencialidad, integridad y disponibilidad.
De acuerdo con la clasificación otorgada al activo ICFE establecerá los niveles de acceso, restricciones o permisos autorizados a los documentos físicos y digitales, sistemas de información y/o cualquier aplicativo que contenga el activo de información con el fin de preservar su confidencialidad, integridad y disponibilidad.

Toda la información debe ser identificada, clasificada y documentada.

Los usuarios responsables de la información del ICFE, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

10.7.3. Etiquetado de la información

Independientemente de su formato, medio o ubicación, la información se clasificará como **INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA** siguiendo el esquema de clasificación de la información adoptada por ICFE y documentada en el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION.

10.7.4. Transferencia de información

Se debe evitar la divulgación, modificación o eliminación no autorizada de los activos de información que lleguen a afectar cualquiera de las operaciones de ICFE.

Por lo anterior:

- Se debe contar con controles de transferencia formales para proteger el intercambio de información, independientemente del medio de comunicación utilizado; del mismo modo se debe implementar controles para prevenir el acceso no autorizado, la copia, modificación, enrutamiento incorrecto, destrucción y denegación de servicio.
- Se debe establecer acuerdos con terceros para la transferencia segura de información entre ICFE y las partes externas a la compañía (proveedores, aliados y demás terceros).
- Se debe proteger la información incluida en los mensajes electrónicos de acuerdo con el nivel de clasificación que contenga.
- Los propietarios de la información que se requiera transferir son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de acuerdo con la documentación vigente.
- Los acuerdos de transferencia deben en todo caso velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo deben especificar las consideraciones de seguridad y reserva de la información, y las responsabilidades por el mal uso o divulgación de esta.

Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realizará siguiendo el procedimiento establecido por la entidad que solicita la información.

La transferencia de información debe contemplar las siguientes directrices:

- Uso de WebServices, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.

- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
- Informar al titular de los datos, la transferencia de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

10.7.5. Traslado de propiedad

El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica del ICFE, debe ser autorizado por el propietario del activo, previa solicitud del funcionario interesado.

Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones del ICFE, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.

Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos del ICFE, solo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a través del proceso de sanitizacion. La oficina de Informática generará un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas del Instituto.

10.8. CONTROL, DERECHOS DE ACCESO Y GESTIÓN DE IDENTIDADES

Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el propietario de cada activo, según el procedimiento ICFE-P-159 GESTION USUARIOS Y CONTRASEÑAS.

Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad Informática del ICFE debe estar autorizado por la oficina de Informática.

Todas las conexiones remotas deben ser autenticadas y seguras antes de conceder el acceso, el tráfico de datos debe estar cifrado.

La creación, modificación, y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática debe seguir el procedimiento ICFE-P-159 GESTION USUARIOS Y CONTRASEÑAS.

Todo usuario que se cree para que un tercero ingrese a la red del ICFE, debe tener una fecha de vencimiento específica, la cual en ningún caso debe superar la fecha de terminación de sus obligaciones contractuales.

La asignación de privilegios en las aplicaciones para los diferentes usuarios estará determinada por el procedimiento ICFE-P-159 GESTION USUARIOS Y CONTRASEÑAS. Estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

Los equipos de terceros que requieren acceder a la red del ICFE, deben cumplir un procedimiento de sanitización informática antes de concedérseles dicho acceso.

Cuando exista la necesidad de otorgar acceso de terceras partes al ICFE, debe realizarse siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre los siguientes aspectos:

- El tipo de acceso requerido (Físico, lógico y a que recurso).
- Los motivos para los cuales solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte

10.9. INFORMACIÓN DE AUTENTICACIÓN Y USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS

Para garantizar la autenticación adecuada de ICFE en los diferentes sistemas de información y evitar fallas en los procesos de autenticación se debe garantizar que:

a) Las contraseñas generadas automáticamente durante los procesos de inscripción en los sistemas de información son únicas para cada persona, y los usuarios realizan el cambio después del primer uso.
b) La información de autenticación predeterminada, predefinida o proporcionada por los proveedores debe siempre que sea posible, cambiarse inmediatamente después de la instalación de sistemas o software.
c) Cada Colaborador de ICFE le será asignado su propio usuario y clave de acceso a sistemas y/o aplicaciones, los permisos dentro de ellos serán definidos de acuerdo con su perfil, autorizados por la línea de supervisión del área a la que pertenezca y el Oficial de Seguridad de la información.
d) Se parametrizará cada aplicativo y recurso Informático de ICFE para que solicite claves con alta complejidad. (Mínimo 8 caracteres, mayúsculas, minúsculas, números y signo)
e) Se utilizan mecanismos de auditoría operativa para controlar la utilización de los accesos a las aplicaciones y asegurar que el nivel de acceso otorgado sea consistente con las funciones de cada usuario.

La administración, así como la asignación y entrega de las contraseñas a los usuarios debe seguir el procedimiento ICFE-P-159 GESTION USUARIOS Y CONTRASEÑAS. Los

usuarios deben seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

1. Las contraseñas son de uso personal y por ningún motivo se deben prestar a otros usuarios.
2. Las contraseñas no deben ser reveladas.
3. Las contraseñas no se deben escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento ICFE-P-159 GESTION USUARIOS Y CONTRASEÑAS.
4. Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que una persona esté utilizando un usuario y contraseña que no le pertenece, de acuerdo con el procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS.

10.10. SEGURIDAD DE LA INFORMACIÓN CON PROVEEDORES

Se debe establecer con los proveedores que tenga acceso a los activos de información de ICFE, acuerdos que relacionen los requisitos de seguridad de la información pertinentes respecto al acceso, procesamiento, y almacenamiento de la información. Los acuerdos deben incluir requisitos para tratar los riesgos de seguridad de la información.

Cuando aplique, ICFE exigirá a los proveedores y aliados comerciales, información frente al personal que participará en el contrato o servicio prestado, así como sus perfiles, funciones y responsabilidades, el proveedor está obligado a informar sobre cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación y que puedan afectar la seguridad de la información.

Todo el personal que trabaje en función de la prestación de los servicios de los proveedores o terceros debe cumplir las normas de seguridad de la información establecidas en ICFE; en caso de incumplimiento de las obligaciones del tercero, la compañía se reservará el derecho de veto al personal que haya cometido la infracción, así como la adopción de las medidas sancionatorias que se consideren pertinentes en relación con el proveedor.

Los lineamientos establecidos en esta política cubren a todos los proveedores de ICFE incluyendo los asociados con la cadena de suministro de TICs.

Dentro de la gestión con los terceros se debe:

- Verificar el cumplimiento de los requisitos de seguridad relacionados con la validación de antecedentes, desempeño, capacidad de servicio y demás aspectos de seguridad identificados para el proyecto que se va a ejecutar con un proveedor, aliado o tercero.
- Definir los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de información de ICFE, los planes de tratamiento deben ser acordados y documentados.
- Diligenciar y firmar los acuerdos de confidencialidad y acuerdos de intercambio de información con proveedores. En los casos que aplique subcontratación de personal

o proveedores debe hacerse extensivos los acuerdos de confidencialidad, intercambio de información, políticas y lineamientos de seguridad.

- Establecer acuerdos de nivel de servicio, así como todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de ICFE.
- El responsable del contrato debe hacer seguimiento al cumplimiento contractual y evaluar prestación de servicios de los proveedores.
- Cuando el proveedor sea catalogado como “Crítico” se debe asegurar que al momento de su contratación cuente con planes de continuidad que soporten los servicios proporcionados a ICFE; del mismo modo se solicitarán actualizaciones del documento para cada renovación del contrato u orden de compra.
- Los proveedores se comprometen a comunicar de manera inmediata cualquier incidente, debilidad o amenaza que afecte a ICFE.
- El proveedor debe notificar oportunamente a ICFE cualquier cambio a realizar como parte del producto o servicio. Una vez notificados, se debe ejecutar las acciones necesarias para garantizar que estos cambios no afecten la prestación del servicio.
- ICFE debe realizar seguimiento, revisión y auditoría a los proveedores “Críticos” que hagan uso de sus activos de información, con el fin de detectar oportunamente desviaciones en el cumplimiento de las políticas y controles previamente establecidos.
- En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones del ICFE, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.
- En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicio críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.
- El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la oficina de Informática, aprobarán y autorizarán el acceso y uso de la información.
-

10.11. SEGURIDAD DE LA INFORMACIÓN PARA EL USO DE SERVICIOS EN LA NUBE

Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos.

Ningún servicio de carácter operativo e institucional del ICFE debe ser contratado en servicios en la nube público o hibrido.

Se podrá implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.
El uso de servicios en la nube implica una responsabilidad compartida en relación con la seguridad de la información un esfuerzo de colaboración entre el proveedor del servicio en

la nube e ICFE, un acuerdo de servicio en la nube debe abordar los requisitos de confidencialidad, integridad y disponibilidad. Adicionalmente, debe contar con la definición clara de los niveles de servicio y objetivos propuestos.

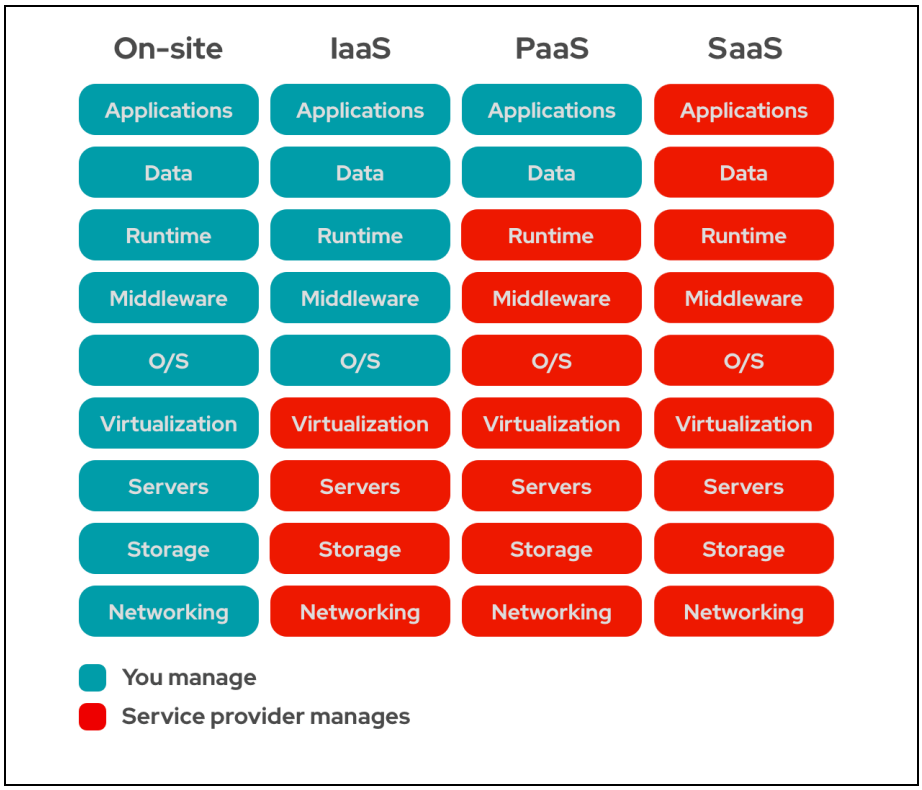

Figura no.1 Servicios onpremise, IAAS, PAAS, SAAS
(Tomado de https://www.redhat.com/es/topics/cloud-computing/iaas-vs-paas-vs-saas)

Por lo anterior:

a) Para todos los servicios en la nube, ICFE debe revisar los acuerdos de servicios con los proveedores, garantizando la implementación de requisitos de seguridad de la información.
b) Definir funciones y responsabilidades relacionadas con el uso y gestión de los servicios en nube.
c) Mantener información disponible para que el personal de ICFE sepa cómo administrar las capacidades de seguridad de la información proporcionadas por el proveedor.
d) Identificar y gestionar los riesgos de seguridad de la información para servicios en nube.
e) Implementar controles de seguridad de la información para gestionar los servicios de nube prestados por el proveedor, por ejemplo: Segregación de ambientes y controles de acceso a microservicios disponibles en ambiente productivo.
f) Cualquier riesgo residual que exceda el apetito de riesgo de ICFE, relacionado con el uso de servicio en la nube debe ser identificado y aceptado por el Comité designado para el monitoreo y control del SGSI.
g) Se debe revisar que, en el contrato con los proveedores de nube, se encuentren estipuladas las responsabilidades de cada una de las partes.

h) Cuando existan interfaces entre diferentes proveedores de servicios en nube en los cuales ICFE requiere el intercambio de información, esta debe estar cifrada y la conexión entre los proveedores de servicios se debe realizar mediante una autenticación y autorización apropiada.
i) Cuando se requiera la implementación de un cambio en diferentes proveedores de servicios en nube se debe contar con un procedimiento de Control de cambios definido al interior de ICFE.

(*) Si el proveedor de nube es SaaS, la mayoría de los controles de seguridad son responsabilidad del tercero, razón por la cual ICFE debe validar el cumplimiento de estos a través de los certificados proporcionados por este y los niveles de disponibilidad del servicio, así como a través de la implementación de controles de gestión de usuarios y protección de la información y de los canales que permiten la comunicación segura con el proveedor.
(**) definir los criterios de selección que apliquen de acuerdo con el tipo y alcance de uso del servicio en la nube a contratar

10.12. PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los funcionarios y terceros deben informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS.

Para los casos en que los incidentes reportados requieran judicialización, se debe coordinar con los organismos que cuentan con función de policía judicial.

Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS para la Institución.

Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo, y de ser posible, la valoración de los daños.

Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

Los resultados de las investigaciones que involucren a los funcionarios del ICFE deben ser informados a las áreas de competencia.

La oficina de Informática debe establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

10.13. EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información debe determinar si el evento reportado corresponde con un incidente de seguridad de la información de acuerdo con los criterios establecidos por ICFE relacionados en el Procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS, del mismo modo se debe determinar la clasificación o taxonomía del incidente.

10.14. RECOPILACIÓN DE EVIDENCIA

ICFE debe desarrollar actividades para la recolección de evidencia durante la gestión del incidente, la cual podrá ser utilizada cuando se requieran acciones disciplinarias o acciones legales, en cuyo caso se contratará un experto forense.
La evidencia recolectada no debe ser manipulada y debe cumplir con los requisitos legales correspondientes.

10.15. APRENDIZAJE SOBRE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se debe documentar para cada uno de los incidentes presentados las lecciones aprendidas, con el fin de contar con una base completa de conocimiento que le permita analizar, recopilar, cuantificar y monitorear la información, así como establecer las actividades para resolver incidentes similares en el futuro.
Del mismo modo la base de lecciones aprendidas permitirá capacitar al personal involucrado con ejemplos claros de lo que puede suceder, como responder a los incidentes y que acciones se debe implementar para evitar su materialización en el futuro.

10.16. SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN

La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

El plan de continuidad de negocio debe desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos críticos luego de una interrupción o falla. La seguridad de la información debe restaurarse al nivel requerido y en los plazos establecidos por el negocio.

ICFE debe disponer de controles de seguridad y herramientas de apoyo con el fin de mantener la seguridad y continuidad de los procesos críticos.

Para el ICFE, su activo más importante es el recurso humano, y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionadas con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio.

Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.

En el proceso de identificación de riesgos de continuidad de negocio deben ser considerados los riesgos de disponibilidad, confidencialidad e integridad para los escenarios que pudiesen llegar a presentarse, con el fin de garantizar la existencia de estos tres pilares durante la ejecución de cualquier proceso contingente.

10.17. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

ICFE debe documentar, probar y revisar los procesos, procedimientos y controles de seguridad con el fin de garantizar el cumplimiento de los objetivos de la compañía durante cualquier interrupción, crisis o desastre que pudiera llegar a presentarse, afectando la ejecución de los procesos críticos del negocio, para esto se debe asegurar el diseño y definición de:

a) Una estructura organizacional que permita prepararse, responder y mitigar las consecuencias de una interrupción a través del apoyo de personal con las responsabilidades, habilidades y competencia necesarias.

b) Un Business impact Analysis – BIA que le permitirá identificar los procesos críticos de negocio y sus necesidades respecto a:

   - Tiempos y puntos objetivos de recuperación.
   - Aplicaciones y servicios tecnológicos requeridos.
   - Dependencia de información, funcionarios y elementos de soporte.
   - Dependencia de proveedores.

c) Planes de continuidad de negocio, procedimientos de respuesta y recuperación los cuales son:

   - Probados y actualizados con una periodicidad anual.
   - Aprobados por el Comité designado para el monitoreo y control del SGSI.

d) La definición del plan de recuperación de desastres (DRP), que incluye:

   - El cumplimiento de los requisitos y objetivos de continuidad de negocio tal y como se especifica en el Business impact Analysis - BIA
   - RTO de cada servicio de TI priorizado, así como los procedimientos operativos que permitan restablecer cada componente.
   - RPO de cada servicio y los procedimientos para restaurar la información requerida.
   - Procedimientos técnicos, identificación y tratamiento riesgos, escenarios y estrategias tecnológicas.

10.18. REQUISITOS LEGALES, ESTATUTARIOS, REGLAMENTARIOS Y CONTRACTUALES

ICFE asegurara el cumplimiento de las directrices contenidas en la legislación regional, por lo que se compromete a verificar todos los acuerdos contractuales, normas, leyes y estatutos relacionados con seguridad de la información y ciberseguridad;

La normatividad existente debe tenerse en cuenta cuando:

e) Se desarrollen políticas, manuales y procedimientos de seguridad de la información en donde ICFE identifica toda la legislación pertinente a la seguridad de la información para su tipo de negocio.
f) Se diseñen, implementen, ejecuten o sucedan cambios en los controles de seguridad de la información.
g) Se clasifiquen los activos de información y se establezcan requisitos de seguridad de acuerdo con los requisitos internos o de terceros.
h) Se evalúen los riesgos de seguridad de la información y ciberseguridad y se determinen los planes de tratamiento.
i) Se determinen los requisitos contractuales con las partes interesadas y el alcance de los servicios.
j) Se realice cifrado, se gestionen llaves, firmas digitales, sellos y certificados.

ICFE debe revisar periódicamente cualquier cambio en la legislación, con el fin de mantenerse al día con las nuevas regulaciones, documentando procesos y responsabilidades individuales para cumplir con los requisitos establecidos por la normatividad.

El ICFE deberá garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales, y propender por la seguridad de la información ingresada a través de ellos, aclarando que no es responsable de la veracidad de esta.

10.19. DERECHOS DE PROPIEDAD INTELECTUAL

El ICFE cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementará los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

No se permitirá el almacenamiento, descarga de internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

Se permitirá el uso de documentos, cifras y/o textos de carácter público, siempre y cuando se cite el autor de estos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

El software a la medida, adquirido a terceras partes o desarrollado por funcionarios del ICFE, serán de uso exclusivo del Instituto y la propiedad intelectual será de quien lo desarrolle.

10.20. GESTIÓN DE DOCUMENTOS Y PROTECCIÓN DE REGISTROS

ICFE debe establecer lineamientos y actividades con el fin de proteger la autenticidad, confiabilidad, integridad y usabilidad de los documentos y registros de la compañía, durante su gestión, almacenamiento, cadena de custodia y eliminación en el tiempo en que estos sean utilizados.

10.21. PRIVACIDAD Y PROTECCIÓN DE PII (INFORMACIÓN DE IDENTIFICACIÓN PERSONAL)

ICFE está comprometida con la protección de la privacidad y seguridad de los datos personales de sus colaboradores, clientes, proveedores y demás titulares, dando cumplimiento a la legislación vigente sobre la protección de datos personales. ICFE divulga su “Política de tratamiento de datos personales” a través de la página web para conocimiento de todas las partes interesadas relevantes, donde se contemplan las responsabilidades, las finalidades para el uso de los datos personales recolectados, los derechos de los titulares y los mecanismos para ejercer sus derechos; Adicionalmente, cuenta con las autorizaciones correspondientes de los titulares para el tratamiento de sus datos personales.

10.22. REVISIÓN INDEPENDIENTE DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información y su implementación, objetivos de control, controles, políticas, procesos y procedimientos, se deben revisar independientemente a intervalos planificados (por lo menos anualmente), o cuando ocurran cambios significativos en la implementación de la seguridad, esta actividad debe ser ejecutada por auditoría interna o una compañía de tercera parte especializada en tales revisiones. Los auditores que llevan a cabo estas revisiones deben tener la independencia, experiencia y las habilidades adecuadas para emitir informes que generen valor a la compañía. Por lo que se deben tener en cuenta para estas revisiones:

a) Los sistemas de información, red de trasmisión de datos, las aplicaciones y sistemas operativos serán revisados para determinar el cumplimiento de las directrices de seguridad de la información y hacer seguimiento a las estrategias de mitigación en caso de identificar vulnerabilidades o brechas que deban ser remediadas.
b) Los resultados de las revisiones deben ser presentados al Comité designado para el monitoreo y control del SGSI, así como los planes de remediación y las debilidades recurrentes en el ambiente de control.

c) El seguimiento oportuno a las no conformidades o acciones de mejora y la necesidad de cambio en el enfoque de la seguridad de la información.

Se debe realizar revisiones adicionales cuando ocurran alguna de las siguientes situaciones:

- Leyes y regulaciones que afecten a ICFE.
- Incidentes significativos.
- Nuevos proyectos, productos o servicios.
- Cambios significativos en controles o procedimientos de seguridad de la información.

10.23. CUMPLIMIENTO DE LAS POLÍTICAS, NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Los lideres de procesos y los propietarios de información deben identificar y revisar por lo menos anualmente, el cumplimiento de los requisitos de seguridad de la información, para esto deben notificar los niveles de cumplimiento de los requisitos de seguridad de la información; si se identifican incumplimientos se debe asegurar:

a) La identificación de las causas generadoras del incumplimiento.
b) La implementación de acciones correctivas apropiadas.
c) La verificación de las acciones correctivas de acuerdo con los tiempos de remediación definidos con el fin de verificar su efectividad o identificar cualquier deficiencia o debilidad adicional.
d) La documentación y conservación de la evidencia y los resultados de las mediciones, los registros deben mantenerse sin excepción y se pondrán a disposición de cualquier ente regulatorio, auditoría interna o de control.

(*) Cuando se requiera el área legal apoyará a ICFE en el levantamiento o identificación de nueva normatividad o requisitos adicionales de seguridad que requieran ser implementados.

10.24. PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS

La ejecución de cualquier actividad compleja que requiera soporte documental o que pueda materializar un riesgo si no se realiza correctamente en el procesamiento de información, comunicaciones y seguridad informática debe estar respaldada por instrucciones o procedimientos operativos documentados. Estos documentos deben estar siempre disponibles para todos los usuarios que los necesiten en el desarrollo de sus labores.

Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contacto de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por el administrador de la aplicación, propietario del activo, jefe de dependencia o el funcionario a quien se le hayan otorgado dichas funciones.

Los procedimientos operativos deben contener instrucciones para el manejo de los errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

Los procedimientos establecidos deben ser revisados y actualizados periódicamente o cuando ocurran cambios significativos en los procesos de ICFE.

11. CONTROLES SOBRE PERSONAS

11.1. VERIFICACIÓN DE ANTECEDENTES

ICFE debe establecer un conjunto de controles entorno a la selección de personal, como:

- La idoneidad y competencia del candidato para desempeñar las funciones de la vacante.
- La verificación de antecedentes en el proceso de selección y vinculación de nuevos colaboradores en línea con los riesgos asociados a la seguridad de la información.

Adicionalmente se realiza un análisis de cada cargo, tomando en consideración los accesos y privilegios requeridos sobre los activos de información y su clasificación en términos de criticidad y sensibilidad, cuando se determina que el cargo evaluado es crítico para la compañía, se realizará un estudio de seguridad con el fin de comprobar la idoneidad del empleado a contratar.
Algunas verificaciones que se deben tener en cuenta de acuerdo con el rol a desempeñar sin limitarse a estas son:

- Referencias laborales y personales.
- Integridad y veracidad de la hoja de vida.
- Certificados académicos.
- Certificaciones profesionales.
- Verificación de la identidad (ID, CC o pasaporte).
- Antecedentes Judiciales o penales.
- Verificación en listas restrictivas.
- Estudio de seguridad (Cuando aplique).

Las verificaciones sobre antecedentes se deben realizar previo a la vinculación y para colaboradores a término indefinido, fijo, temporales y contratistas.
ICFE evaluará mínimo cada tres años, los antecedentes y certificaciones de los colaboradores críticos, con el fin de confirmar la idoneidad continua del personal vinculado.

Los soportes sobre la verificación de antecedentes y validaciones efectuadas contarán con las autorizaciones y controles de seguridad requeridos por el sistema de gestión de privacidad y protección de datos personales.

(*) Cuando los colaboradores sean contratados a través de proveedores de servicio, los requisitos de selección deben incluirse en los acuerdos contractuales.

11.2. TÉRMINOS Y CONDICIONES DE EMPLEO

Las funciones y responsabilidades en materia de Seguridad de la información deben estar incorporadas en la descripción del cargo que desempeña cada empleado. Es una obligación de los colaboradores y contratistas aplicar sin excepción las políticas de Seguridad de la Información, así como: conocer, respetar, cumplir y hacer cumplir las políticas, procedimientos y lineamientos de seguridad definidos en este manual y acatar las leyes, decretos y regulación establecida por entes de control.

Para esto ICFE debe realizar las siguientes acciones:

a) En la vinculación de personal independientemente de la modalidad de contratación, se debe suscribir un compromiso de cumplimiento de las políticas de seguridad de la información.

b) La Gerencia responsable debe proveer los medios necesarios para establecer planear, desarrollar, ejecutar y mantener programas de sensibilización en seguridad de la información, tomando en consideración los roles y responsabilidades definidos en ICFE.

c) Se establecerán acuerdos de confidencialidad con colaboradores y contratistas en el momento de la vinculación laboral o contractual donde se establece el tiempo de duración de estos durante y luego que haya finalizado la relación laboral/contractual.

d) Los términos y condiciones relacionados con seguridad de la información se revisarán y actualizarán si se requiere cuando se presenten cambios en las leyes y políticas.

(*) Si el empleado incurre en una violación a las políticas de seguridad de la información, será tratado de acuerdo con un proceso disciplinario.

11.3. CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Se debe mantener un programa anual de concientización y capacitación para todos sus funcionarios, así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades dentro del Instituto.

Todos los funcionarios y terceros al servicio del ICFE, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos

necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

11.4. PROCESO DISCIPLINARIO

El incumplimiento de los lineamientos definidos en el presente documento tendrá como resultado la aplicación de sanciones conforme a la magnitud y características de la violación. Se incluyen dentro del proceso disciplinario las acciones a emprender cuando un empleado o parte interesada relevante comete una violación a la seguridad de la información, para esto ICFE definió el procedimiento ICFE-P-18 GUÍA PARA LAS INVESTIGACIONES DISCIPLINARIAS.

- Un procedimiento disciplinario en el que categoriza las violaciones de seguridad por nivel de criticidad, consecuencia y las acciones disciplinarias a seguir.
- El procedimiento debe considerar agravantes como la reincidencia, si el empleado o parte interesada había recibido capacitaciones previamente o si la violación corresponde con un acto intensional o no intensional.

(*) El procedimiento disciplinario no puede iniciar, si no se cuenta con la evidencia suficiente que permita determinar que se ha presentado por parte del empleado o parte interesada relevante, una violación a las de Políticas de Seguridad de la Información. El procedimiento disciplinario debe cumplir con los requisitos legales y contractuales requeridos.

11.5. RESPONSABILIDAD DESPUÉS DE LA TERMINACIÓN O CAMBIO DE EMPLEO

La terminación o cambio laboral será coordinada por el área de talento humano. En la terminación laboral se debe asegurar la devolución de los activos asignados al personal y la inactivación de las cuentas de acceso a los recursos y aplicativos como mínimo en el último día laboral.

Al momento de la desvinculación o de cambio de roles, todo funcionario y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados. Esto mediante un formato establecido por la oficina de Informática del ICFE.

11.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

Todos los empleados públicos y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que debe ser parte integral de los contratos, utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

Los acuerdos de confidencialidad de la información son revisados cada vez que se presente algún incidente de seguridad y/o que el Oficial de Seguridad de la Información lo requiera necesario, con el fin de actualizar las obligaciones y compromisos definidos. Para la firma

de los acuerdos de confidencialidad, se deben tener en cuenta como mínimo los siguientes aspectos:

a) Ser suscritos por colaboradores con contrato a término indefinido, término fijo, temporales y proveedores.
b) Definir responsabilidades y acciones a seguir para evitar la divulgación de información no autorizada.
c) Documentar clausulas entorno a la propiedad de la información, habeas data, secretos comerciales y propiedad intelectual.
d) Definir los términos para la devolución o destrucción de la información.
e) Documentar el tiempo de vigencia del acuerdo.
f) Cumplir con los términos legales y regulatorios.
g) Definir los derechos a auditar al proveedor.
h) Definir los reportes o informes requeridos para la actividad contratada.

11.7. TRABAJO REMOTO

ICFE debe implementar controles de seguridad para todo el personal que trabaje de forma remota, con el fin de proteger la información a la que se accede, que se procesa o almacena. Por lo anterior se deben contemplar aspectos como:

Realizar una verificación de los equipos asignados a los colaboradores para que cumplan una línea base de seguridad que considere:

- Controles de acceso.
- Herramientas para cifrar la información crítica almacenada en estos.
- Mecanismos de respaldo de la información que contienen.
- Herramientas de seguridad necesarias para mitigar el código malicioso.
- Navegación controlada.
- Herramientas para evitar la fuga de información - DLP.
- Múltiple factor de autenticación.
- Hacer uso de VPN o Firewall.
- bloqueo de sesiones por inactividad.

Todo empleado que utilice su equipo personal para conectarse a la red de ICFE debe entender que su dispositivo es una extensión de la red de la compañía y por tanto aplicarán las mismas políticas y lineamientos existentes.

Todo dispositivo personal que requiera conectarse a la red de ICFE debe contar con la autorización previa del Oficial de Seguridad de la Información quien asegurara que este cuente con las condiciones de seguridad requeridas.

11.8. REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Todos los colaboradores y usuarios deben ser conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.

Los colaboradores y usuarios no están autorizados para probar las vulnerabilidades de seguridad de la información sospechosas y hacerlo puede acarrear un proceso disciplinario y/o responsabilidad legal.

ICFE establece los siguientes mecanismos para realizar el reporte de eventos:

- ICFE HELPDESK (Mesa de servicio).
- Correo electrónico dirigido directamente al Profesional de Seguridad de la información.
- Correos dirigidos al personal de Soporte de primer nivel.

Entre las situaciones que deben reportar los usuarios finales se encuentran entre otras:

- Controles de seguridad ineficaces.
- Errores humanos.
- Incumplimientos a la política de seguridad de la información.
- Incumplimientos a los procedimientos de seguridad física.
- Violaciones de acceso- Contraseñas.
- Vulnerabilidades.
- Sospechas de infección por malware.
- Cualquier anomalía o sospecha que se pueda presentar en las actividades normales o que puedan afectar los activos de información.

Ver Procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS.

12. CONTROLES FÍSICOS

12.1. PERÍMETRO DE SEGURIDAD Y ENTRADA FÍSICA

Se consideran áreas de acceso restringido a todas las áreas donde se encuentran alojados los equipos de procesamiento o almacenamiento de información privada, la infraestructura de soporte a los sistemas de información y comunicaciones, y las áreas donde se encuentra la documentación privada del ICFE; por lo cual se deben emplear mecanismos de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.

No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

Todas las puertas que utilicen sistema de control de acceso deben permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados, evitar que las puertas se dejen abiertas.

La oficina de Informática debe garantizar que el control de acceso al centro de datos del ICFE, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

Todos los funcionarios y contratistas deben portar en un lugar visible el carnet que los identifica como funcionarios o contratistas del Instituto, para el acceso a la Entidad y mientras se encuentre dentro de ella.

Los visitantes deben permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.

Es responsabilidad de todos los funcionarios y terceros, acatar las normas de seguridad y mecanismos de control de acceso al Instituto.

Los funcionarios y terceros, así como los visitantes, deben tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones del ICFE.

Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

Todos los escritorios o mesas de trabajo deben permanecer ordenados y asegurados con el fin de no exponer elementos con información crítica tales como documentos físicos y dispositivos de almacenamiento ante visitantes mal intencionados y de esta forma reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

ICFE, a través de su administración, mantiene un registro de los invitados y colaboradores para garantizar la trazabilidad de cualquier acceso que se presente. Este registro debe ser custodiado con las medidas de seguridad requeridas. Cuando un invitado necesite acceso a las instalaciones, un empleado debe acompañarlo y autorizar su ingreso y salida durante toda la visita.

12.2. ASEGURAMIENTO Y MONITOREO DE OFICINAS, SALAS E INSTALACIONES

Los edificios donde se ejecutan actividades cuentan con sistemas de videovigilancia y circuito cerrado de televisión para registrar y monitorear en línea el acceso a las diferentes áreas de ICFE.

Los sistemas de monitoreo de las oficinas son probados periódicamente con el fin de comprobar que funciona de acuerdo con lo previsto.

No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen del Instituto, a menos que esté autorizado.

La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por la oficina de Informática y exclusivamente con fines institucionales.

12.3. PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

Las áreas de acceso restringido deben contar con mecanismos efectivos que permitan cumplir con los requerimientos ambientales de temperatura y humedad especificados por los fabricantes de los equipos que albergan, y conservación de la documentación que custodia, además de medidas para proteger los equipos del polvo y prevenir amenazas externas como manifestaciones sociales, explosiones en la calle o vandalismo.

Los funcionarios se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a equipos de cómputo, tales como: impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que generen caídas de la energía.

La oficina de Informática deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

Las oficinas de ICFE deben contar con un mapa de riesgos que detalla las amenazas presentes de acuerdo con la ubicación de la infraestructura de TI de ICFE, entre las que se consideran: incendios, inundaciones, terremotos, disturbios civiles, asonadas o cualquier tipo de desastre que pueda ser causado por seres humanos. La evaluación de los riesgos es realizada por el área Riesgos y se encuentran documentadas en la Matriz General de riesgos.

Derivado del análisis de los riesgos identificados, la oficina cuenta con controles físicos y ambientales que impiden el acceso de personal no autorizado y buscan detectar situaciones que atenten contra la vida y la seguridad de los colaboradores, entre los controles implementados se contemplan:

- Alarmas y sistemas contra incendios.
- Extintores.
- Planta y circuitos eléctricos regulados.
- Inspecciones físicas para evitar el ingreso de armas o material peligroso.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del ICFE.
- Cuando se requiera realizar alguna actividad sobre algún armario (*rack*), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.
- Los funcionarios y terceros no deben consumir alimentos ni bebidas en las áreas donde se encuentren activos de información.
- La limpieza y aseo del centro de datos estará a cargo de la oficina de Informática. Esta labor no será realizada por ninguna otra persona ajena a esta dependencia, con el fin de evitar alguna desconexión en los servicios.

- En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
- El centro de datos debe estar provisto de:
  - ✔ Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
  - ✔ Pisos elaborados con materiales no combustibles.
  - ✔ Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe se redundante para que en caso de falla se pueda continuar con la refrigeración.
  - ✔ Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - ✔ Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
  - ✔ Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

(*) Para mayor detalle del plan de emergencias, se debe consultar la información del Sistema de Gestión de seguridad y salud en el trabajo

12.4. ESCRITORIO Y PANTALLA DESPEJADA

En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar los medios que contengan información crítica, protegida bajo llave.

Los usuarios deben bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

Todas las estaciones de trabajo deben usar únicamente el papel tapiz y el protector de pantalla establecido por el Instituto.

Los usuarios no deben almacenar en el escritorio de sus estaciones de trabajo, documentos, accesos directos a los mismos o a sistemas de información sensibles.

Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

ICFE debe contar con una política en el directorio activo que controle el tiempo máximo de inactividad del usuario, cuando esto ocurra la sesión será bloqueada y el funcionario debe ingresar nuevamente sus credenciales para poder acceder al equipo.

Los colaboradores deben asegurar que todo documento que sea impreso debe ser recogido y almacenado inmediatamente, con el fin de evitar que usuarios no autorizados tengan acceso a la información, adicionalmente ICFE cuenta con el uso de credenciales para hacer uso de los medios de impresión.

12.1. UBICACIÓN Y PROTECCIÓN DEL EQUIPO

Los equipos de cómputo deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado, cuando los funcionarios realicen trabajo remoto los equipos debe contar con controles para protección de la información como:

- Controles criptográficos seguros a la fecha, según el NIST (Instituto Nacional de Normas y Tecnología), los siguientes: AES 256; RSA 2048-4096; SHA2/3; DSA/D-H 2048/224 y ECC NIST 192p-512p.
- Los equipos son de responsabilidad estricta de cada colaborador, garantizando que ninguna persona no autorizada pueda acceder al equipo y a la información asignada.
- Cada colaborador debe asegurar que se mantengan las condiciones ambientales y físicas adecuadas para proteger el equipo y preservar la información en el almacenada.

12.2. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones del ICFE, deben velar por la protección de estos, sin dejarlos desatendidos, comprometiendo la imagen o información del Instituto.

El propietario del activo, con el apoyo de la oficina de Informática, identificará mediante una tecnología de análisis de riesgos; las vulnerabilidades potenciales que puede generar el retiro de equipos o medios, de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la defensa y la seguridad nacional, se debe realizar inmediatamente el respectivo reporte, de acuerdo con el procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS, y se debe poner la denuncia ante la autoridad competente, si aplica.

Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del ICFE, deben contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o que puedan poner en riesgo la información que contiene.

ICFE mantendrá un registro para identificar la cadena de custodia del equipo cuando estos son transferidos entre diferentes personas, la información que no necesita transferirse con el activo debe eliminarse de forma segura de acuerdo con los lineamientos establecidos en el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION.

12.3. MEDIOS DE ALMACENAMIENTO

Se restringe la conexión no autorizada a la infraestructura tecnológica del ICFE, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos.

La oficina de Informática, con debida autorización del director del ICFE definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser requerido para el cumplimiento de sus funciones.

Cada medio removible de almacenamiento debe estar identificado de acuerdo con el tipo de información que almacene, dando cumplimiento a los lineamientos establecidos en el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION. Si un medio removible llegase a contener información con distintos niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.

Para los procesos de baja, de reutilización o de garantía de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. La destrucción segura se documentará mediante acta, registro fílmico y fotográfico.

El tránsito o préstamo de medios removibles debe ser autorizado por el propietario de dicho activo.

12.4. SERVICIOS EXTERNOS DE APOYO

Las áreas en donde se realicen operaciones críticas del negocio Centro de Procesamiento de Datos y las oficinas cuentan con contratos y acuerdos de disponibilidad con el tercero contra fallas en el suministro de energía y otras anomalías causadas por los servicios de suministro.

Adicionalmente se debe garantizar que los proveedores de servicios externos cuenten con circuitos alternos y equipos de respaldo de suministro de energía y demás controles que permitan la correcta prestación de los servicios contratados.

12.5. SEGURIDAD EN EL CABLEADO

Se debe garantizar que las líneas eléctricas y de telecomunicaciones donde se ejecuten actividades de ICFE sean protegidas contra interceptaciones, interferencias o daños, para esto se debe asegurar de parte de la administración del edificio que:

a) Que las líneas eléctricas y de telecomunicaciones sean subterráneas o cuenten con canaletas que aseguren la protección del cableado.
b) Separar los cables de comunicación de los cables de potencia con el fin de evitar interferencias, asegurando que cuenten con blindaje electromagnético.
c) Se mantenga el acceso controlado a los centros de cableado (paneles de conexión y a dispositivos de telecomunicaciones), estos elementos deben permanecer en un cuarto cerrado y con los controles de acceso y ambientales requeridos.
d) Etiquetar los cables de extremo a extremo con el fin de mantener detalles suficientes del origen y destino.
e) Qué la distribución del cableado a los puntos de los usuarios finales esté oculta y protegida contra acceso no autorizado.

12.6. MANTENIMIENTO DE EQUIPOS

Solo el personal de soporte técnico está autorizado para realizar mantenimiento a los equipos de cómputo de ICFE, para esto el área de soporte técnico generará los planes de mantenimiento preventivo y correctivo sobre todos los equipos críticos y se deben mantener registros y evidencia de su ejecución.

Las tareas que se deben realizar a nivel de hardware son las siguientes:

a) Limpieza de los dispositivos hardware.
b) Reemplazo o reparación de componentes que no funcionan o están en mal estado.
c) Estas actividades se deben realizar de acuerdo con las sugerencias y buenas prácticas definidas por el fabricante, si el mantenimiento se realiza con un proveedor externo se deben documentar acuerdos de confidencialidad que protejan la información en algunos casos accedida.
d) Cada vez que se realice un mantenimiento de software, se debe autorizar el acceso del empleado o proveedor por el responsable del activo.
e) Si se requiere trasladar el equipo para el mantenimiento, este debe cumplir con las medidas de seguridad requeridas para impedir el acceso a la información en el almacenada.
f) Al recibir el activo, el responsable del equipo debe asegurar su funcionamiento y verificar que este no haya sido manipulado por el proveedor externo.
g) Aplicar medidas para eliminación segura o la reutilización de equipos.

12.7. DISPOSICIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS

Para evitar la fuga de información de los equipos que se desecharán o reutilizarán, los elementos del equipo que contengan medios de almacenamiento deben verificarse para garantizar que todos los datos internos, confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Las etiquetas y marcas que identifiquen a ICFE o que identifiquen la clasificación, el propietario, el sistema o la red deben eliminarse antes de su disposición final, incluida la reventa o donación.
El equipo dañado que contenga medios de almacenamiento puede requerir un análisis de riesgos para determinar si necesita ser reparado o destruido (esto debido a la criticidad de la información en el contenida).

13. CONTROLES TECNOLÓGICOS

13.1. DISPOSICIÓN DE PUNTO FINAL

Los dispositivos de computación móvil de ICFE como equipos portátiles, teléfonos móviles, tabletas, entre otros, son proporcionados por la compañía.

Los colaboradores serán los responsables de garantizar la protección de los equipos asignados, previniendo la materialización de amenazas ambientales presentes en el entorno.

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, la compañía debe implementar controles de acceso como credenciales para el ingreso, tiempo de inactivación de sesiones, técnicas de cifrado sobre la información crítica almacenada en estos, mecanismos de respaldo de la información, instalación y actualización de software, filtrado web y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

Los equipos de computación móvil que se conecten a activos críticos de la infraestructura tecnológica de la compañía son proporcionados por ésta. En cualquier caso, los dispositivos deben contar con las herramientas de seguridad necesarias para mitigar el contagio con código malicioso que garanticen la Seguridad de la Información que contienen.

13.2. DERECHOS DE ACCESO PRIVILEGIADO

El uso de privilegios especiales en los recursos informáticos debe ser restringido y controlado. Los usuarios privilegiados de los recursos informáticos deben ser autorizados por el propietario del activo y por el Oficial de Seguridad de la información. Para la gestión de accesos privilegiados se debe tener en cuenta actividades como:

a) Informar al usuario con acceso privilegiado sobre las responsabilidades asociadas a este tipo de usuario y la necesidad de utilizar controles adicionales para la autenticación de este. (MFA si aplica).
b) Verificar que durante cualquier cambio de rol en ICFE, los usuarios que tienen asignados accesos privilegiados, los requieran de acuerdo con sus nuevos roles y responsabilidades.
c) Cuando se requiera ejecutar cambios o mantenimientos que necesiten accesos privilegiados sobre la infraestructura tecnológica de ICFE, estos deben ser asignados, estar limitados a la ventana de tiempo establecida para la ejecución de la actividad.

d) Registrar todos los eventos generados por cuentas de acceso privilegiado, con el fin de mantener la trazabilidad sobre las acciones ejecutadas por este tipo de usuarios para posibles ejercicios de auditoría.
e) Controlar el bloqueo oportuno de usuarios con acceso privilegiado cuando estos salgan de vacaciones, se retiren de la compañía o cambien de rol.
f) Las cuentas con accesos privilegiados deben ser asignadas a un único usuario responsable de la misma.
g) Los funcionarios de ICFE cuentan con un usuario de red para cualquier actividad del día a día, si se requiere el uso de una cuenta privilegiada, se le debe crear un usuario adicional en donde únicamente se ejecuten las tareas de administración de la plataforma tecnológica.

Ver Procedimiento Control de Acceso

13.3. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

El acceso a la información y otros activos debe considerar aspectos como:

a) Impedir el acceso a información confidencial por parte de usuarios con identidades desconocidas de acuerdo con la clasificación definida la Procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION.
b) El acceso público o anónimo solo debe otorgarse a lugares de almacenamiento que no contengan información confidencial.
c) Controlar a que información puede acceder un usuario, otorgando solo los derechos de acceso requeridos con base en las responsabilidades de su cargo, necesidad de uso, segregación de funciones y principio de mínimo privilegio.
d) Proporcionar controles de acceso físicos o lógicos para asilar información, sistemas, aplicaciones y servicios.
e) Cualquier perfil para asignar en ICFE, debe ser aprobado por el propietario del activo y por Oficial de Seguridad de la Información.
f) Controlar los privilegios asignados sobre grupo de identidades o perfiles como: lectura, escritura, eliminación y ejecución.
g) Implementar técnicas y controles para proteger información crítica de ICFE, entre las actividades que se deben realizar se encuentran:

- Limitar el personal que puede acceder y compartir la información (interna y externamente).
- Generar alertas sobre cambios no autorizados a la información, copias o distribución la misma.
- Monitorear la información y cualquier evento relacionado con posible fuga de esta.
- Mantener trazabilidad de la gestión de cambios sobre la información.
- Para que los usuarios tengan acceso a la información ubicada en las unidades de red o carpetas virtuales, el jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la oficina de Informática del ICFE. Los usuarios tendrán permisos de escritura, lectura o modificación de información en las unidades de red, dependiendo de sus funciones y su rol.

13.4. ACCESO AL CÓDIGO FUENTE

El acceso al código fuente de los programas y elementos como diseños, especificaciones, planes de verificación y validación debe ser confidencial y solo deben tener acceso los usuarios que por su rol y privilegios se encuentren autorizados. ICFE en caso de requerir debe implementar controles de acuerdo con la criticidad de la información gestionada como Múltiple Factor de autenticación y/o VPN.

Adicionalmente se debe considerar los siguientes lineamientos sobre bibliotecas y código fuente con el fin de reducir errores o corrupción sobre el mismo:

a) Uso e implementación de una herramienta para controlar el almacenamiento y versiona miento del código fuente.
b) Implementar controles de acceso sobre el código fuente para asegurar que la lectura, escritura, eliminación y ejecución se encuentren permitidos únicamente a los usuarios autorizados y de acuerdo con su rol y responsabilidad.
c) Cualquier actualización o modificación al código fuente debe ser aprobado a través del proceso de control de cambios.
d) No se debe otorgar acceso directo a los desarrolladores al repositorio de código fuente, sino a través de herramientas que controlen las actividades por ellos ejecutadas.
e) La herramienta para la gestión del código fuente debe mantener un registro de auditoría de todos los accesos y los cambios realizados sobre el mismo.

13.5. AUTENTICACIÓN SEGURA

Dependiendo de la información a la que se accede, ICFE debe implementar diferentes mecanismos de autenticación como son: contraseñas, certificados digitales, tokens, MFA y/o controles biométricos.

Para lo anterior se deben considerar los siguientes lineamientos durante el proceso de autenticación en las aplicaciones de ICFE:

a) No se proporcionará ningún tipo de información como acceso a módulos y funcionalidades de forma previa al inicio exitoso de sesión.
b) Se solicita el restablecimiento de la contraseña por número de intentos fallidos.
c) No se proporcionan mensajes de ayuda durante el proceso de inicio de sesión que ayuden a un usuario no autorizado.
d) Validar la información de inicio de sesión solo al completar todos los datos de entrada.
e) No mostrar, transmitir y almacenar la contraseña de la aplicación en texto claro.
f) Finalizar las sesiones luego de comprobar la inactividad del usuario por un periodo de tiempo definido.
g) En los casos en que sea posible se debe registrar la fecha y hora de última conexión y el dispositivo desde el que se realizó la misma.

13.6. GESTIÓN DE LA CAPACIDAD

La oficina de Informática, como área responsable de la administración de la plataforma tecnológica, debe implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de

procesamiento y comunicación, conforme a lo establecido en el procedimiento ICFE-P-158 GESTION DE LA CAPACIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN.

13.7. PROTECCIÓN CONTRA MALWARE

Los sistemas operacionales y aplicaciones deben actualizarse según lo definido en los procedimientos ICFE-P-156 GESTION DE VULNERABILIDADES TÉCNICAS y ICFE-P-157 CONTROL DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN.

Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deben estar protegidos mediante herramientas de software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

Las herramientas y demás mecanismos de seguridad implementados no deben ser deshabilitados o desinstalados sin autorización de la oficina de Informática; y deben ser actualizados periódicamente.

No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación, diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

Todos los medios de almacenamiento que se conecten a equipos de la infraestructura tecnológica del ICFE, deben ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

La oficina de Informática será responsable de que los usuarios del ICFE mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

Los sistemas, equipos e información institucionales deben ser revisados periódicamente para verificar que no haya presencia de código malicioso.

Implementar reglas o controles de listas de aplicaciones y sitios web, para que se bloqueé el acceso de los usuarios.

El área de TI definirá y mantendrá actualizada una lista de software autorizado a ser instalado en los equipos de cómputo (línea base de software).

Para el uso de la herramienta antimalware ICFE debe contemplar las siguientes consideraciones:

a) Defensa en profundidad: no solo tiene en cuenta el análisis y detección en servidores y equipos de usuario final sino, por ejemplo: correo electrónico, transferencias de archivos entre otros.

b) Cuando el malware sea enviado por un atacante a través de archivos cifrados, estos son analizados en su totalidad por la herramienta, para ejecutar acciones oportunamente.
c) Estar configurada para impedir la desactivación por el usuario final, cuando se requiera cualquier tipo de excepción esta debe estar documentada y aprobada por el Oficial de Seguridad de la Información
d) Definir y actualizar permanentemente los procedimientos para la protección y recuperación de ataques contra malware, ejecutar capacitaciones y generar informes.

Los usuarios finales deben ser capacitados y sensibilizados sobre como identificar y protegerse de archivos o programas infectados con malware.

13.8. GESTIÓN DE VULNERABILIDADES TÉCNICAS

La oficina de informática se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

La oficina de Informática será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica del Instituto.

No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la oficina de Informática, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del ICFE, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.

Se realizará por parte del área competente, el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

La oficina de Informática realizará las revisiones de las alertas de seguridad, definiendo en caso de ser necesario, un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

13.9. GESTIÓN DE LA CONFIGURACIÓN

Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se altere por cambios no autorizados o incorrectos, ICFE debe definir e implementar procesos y herramientas para documentar, mantener y hacer cumplir las configuraciones para hardware, software, servicios (por ejemplo, servicios en la nube), redes, sistemas recién instalados y sistemas operativos durante su vida útil.

Para esto de deben considerar los siguientes aspectos:

a) Definir roles, responsabilidades y procesos para garantizar un control satisfactorio de todos los cambios de configuración, así como su respectivo monitoreo.
b) Definir líneas base de configuración de acuerdo con las buenas prácticas y guías establecidas por proveedores claves.
c) Revisar y actualizar las líneas base de configuración periódicamente, manteniendo información de todas las versiones en uso y asegurando que las plantillas contengan fechas de último cambio, control de versiones, información del elaborador y aprobador del documento.
d) Monitorear periódicamente el cumplimiento de las líneas base de configuración asegurando el grado de implementación para los diferentes servicios y sistemas.
e) La configuración de los equipos siempre debe garantizar el cumplimiento de las leyes y disposiciones de derechos de autor y privacidad de los datos.

Para mantener un nivel base de configuración de seguridad se debe asegurar que se deshabiliten:

- Identidades innecesarias o con derechos de acceso privilegiado que no son requeridas.
- Funciones y servicios innecesarios.
- La posibilidad de configuración de endpoints y relojes de los dispositivos por los usuarios finales.
- Contraseñas y configuraciones predeterminadas o por defecto.

13.10. ELIMINACIÓN DE LA INFORMACIÓN

Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales, la información almacenada en sistemas de información o en cualquier otro medio de almacenamiento debe ser eliminada cuando la ley lo indique, ya no sea necesaria o de acuerdo con los tiempos de retención de esta.
Ver Procedimiento Borrado seguro de la información

13.11. ENMASCARADO DE DATOS

En caso de aplicar ICFE debe limitar la exposición de datos confidenciales asegurando que se cumplan con los requisitos legales, estatutarios, reglamentarios y contractuales, para esto se considerará ocultar los datos confidenciales (Cuando aplique ejemplo: datos de producción utilizados en ambiente de pruebas), mediante el uso de técnicas como el enmascaramiento, seudonimización o anonimización para esto se debe utilizar las siguientes estrategias:

- Cifrado a través del uso de llaves simétricas o asimétricas.
- Anular o eliminar caracteres.
- Cambio en números y fechas o sustitución de información confidencial para evitar la identificación del titular.
- Ocultar valores con su hash.

Cuando se utilicen estas técnicas se debe verificar si los datos han sido adecuadamente anonimizados o seudonimizados.

ICFE limitará el acceso a los datos solo al personal que lo requiere de acuerdo con sus roles y responsabilidades y debe mostrar solo la información mínima requerida para el desempeño de sus funciones.

Adicional al proceso de enmascaramiento de los datos, se validará la implementación de controles como:

a) Controles de acceso a los datos procesados.
b) Acuerdos o restricciones en el uso de los datos.
c) Seguimiento al suministro y recepción de los datos personales tratados.

13.12. PREVENCIÓN FUGA DE DATOS

Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas, ICFE debe considerar los siguientes aspectos para reducir el riesgo de fuga de datos:

a) Identificar, monitorear y detectar información confidencial en riesgo de divulgación no autorizada.
b) Identificar y clasificar la información para protegerla contra fugas (p.ej., información personal, confidencial o de uso interno).
c) Monitorear los canales para prevenir fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos portátiles de almacenamiento).
d) Actuar para evitar que se filtre información (p.ej., poner en cuarentena los correos electrónicos que contengan información confidencial).
e) Se evaluará la posibilidad de restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de ICFE y se revisarán las opciones para detectar y bloquear las acciones de los usuarios o transmisiones de red que expongan información confidencial.
f) ICFE buscará implementar herramientas de prevención de fuga de datos y las configurará para que se evite copiar y pegar información fuera del control organizacional.
g) Cuando se realice una copia de seguridad de los datos, se debe tener cuidado para asegurar que se cuente con los mecanismos de seguridad como cifrado, control de acceso y protección de los medios de almacenamiento.

13.13. COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la oficina de Informática y las dependencias responsables de la misma, contenida en la plataforma tecnológica del ICFE, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el Procedimiento ICFE-P-37 GENERACIÓN DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN.

Los medios de las copias de respaldo se almacenarán tanto localmente como en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

Se debe establecer un plan de restauración de copias de seguridad que será probado a intervalos regulares, establecidos según las necesidades y capacidades del Instituto, con el fin de asegurar que son confiables en caso de emergencia. Estas copias serán retenidas por un periodo de tiempo determinado, de acuerdo a lo establecido en el procedimiento ICFE-P-37 GENERACIÓN DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN.

La oficina de Informática del ICFE, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca de su traslado, frecuencia e identificación; así mismo, definirá conjuntamente con las dependencias usuarias los periodos de retención de dicha información.

Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

13.14. REDUNDANCIA DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN

De acuerdo con la necesidad, ICFE debe documentar e implementar una arquitectura redundante para asegurar la disponibilidad de sus servicios y sistemas de información críticos, para esto se contemplará las siguientes actividades:

a) Los servicios de la compañía que se encuentran contratados con proveedores de nube quienes ofrecen diferentes zonas y regiones para mantener la redundancia y disponibilidad de estos.
b) El proveedor de nube debe proporcionar instancias paralelas de los componentes de software que permiten redireccionar automáticamente el uso de los servicios en caso de ser necesario.
c) El proveedor de nube proporcionará componentes duplicados como, por ejemplo: CPU, discos duros, memorias, switches, routers y conmutadores.
d) Se deben realizar pruebas de continuidad con el fin de confirmar la conmutación sobre los servicios críticos de la compañía.

13.15. ANÁLISIS, PROTECCIÓN DE REGISTROSY ACTIVIDADES DE SEGUIMIENTO

Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento de red y de seguridad informática, deben generar registros de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento Monitoreo y Revisión de Logs.

El tiempo de retención de los Logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.

El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica debe ser reportado a la oficina de Informática, mediante el procedimiento ICFE-P-34 SOPORTE Y ATENCIÓN A INCIDENTES INFORMÁTICOS.

ICFE debe almacenar, proteger, analizar los registros, excepciones y fallas. Para esto debe mantener la integridad de la información registrada a través de la implementación de controles contra el acceso no autorizado a logs y eventos y así poder respaldar cualquier tipo de investigación que se requiera.

a) Para esto ICFE debe conservar la siguiente evidencia:

- Actividades del sistema.
- Fechas, horas, detalles relevantes del evento (como, por ejemplo: inicio y cierre de sesión).
- Identidades del dispositivo y ubicación.
- Direcciones de red y protocolos.

b) Entre los eventos que deben ser analizados sobre sistemas críticos, se encuentran los siguientes:

- Intentos de acceso a los sistemas (exitosos y fallidos).
- Cambios en la configuración del sistema.
- Monitoreo de las acciones de los usuarios privilegiados.
- Utilización de programas de utilidad y aplicaciones.
- Archivos críticos accedidos y eliminados.
- Activación y desactivación de sistemas de seguridad como antivirus y sistemas de detección y protección de intrusos, cortafuegos, y filtrado web.
- Creación, modificación o supresión de identidades.
- Transacciones críticas ejecutadas por los usuarios en las aplicaciones.
- Terminación no planificada de procesos y aplicaciones.
- Escaneo no autorizado de aplicaciones o servicios.

En ICFE, la revisión de registros debe cubrir el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que puedan representar indicadores de compromiso, para esto se deben contemplar los siguientes lineamientos:

- Contar con las habilidades necesarias en el personal encargado de esta función.
- Documentar y revisar los registros o eventos.

- Definir los campos requeridos para cada log.
- Definir y afinar casos de uso que permitan detectar comportamientos anómalos en ICFE y que al correlacionarlos ayuden a identificar posibles incidentes de seguridad.
- Obtener los resultados de los análisis realizados, tendencias o patrones.
- Realizar análisis de inteligencia de las amenazas presentes.
- Realizar el análisis de los logs y las actividades de monitoreo para identificar lo siguiente: intentos exitosos y fallidos para acceder a los recursos como: servidores, DNS, portales web, aplicaciones críticas, tráfico de red, archivos de configuración, entre otros.
- Monitoreo de sistemas de seguridad como antivirus y sistemas de detección y protección de intrusos, cortafuegos, y filtrado web.
- Se monitorean y correlacionan diferentes fuentes de seguridad.
- Se realizan comprobaciones contra código adicionado o agregado en los sistemas.
- La revisión de logs, independientemente de la existencia de reportes de incidentes de seguridad, se realiza con una periodicidad definida o cuando la situación lo amerite.
- El resultado de los riesgos relevantes identificados en los logs se comunica al Comité designado para el monitoreo y control del SGSI.
- La disponibilidad y capacidad de recursos como: CPU, memoria, discos duros, ancho de banda y su rendimiento.

13.16. SINCRONIZACIÓN DEL RELOJ (CLOCK)

Todos los relojes de la infraestructura tecnológica de ICFE deben estar sincronizados con un sistema de referencia estándar que relacione la hora legal del país, de acuerdo con la ubicación del usuario, esta actividad permite que la compañía pueda soportar cualquier investigación sobre incidentes de seguridad de la información.

Adicionalmente y siempre que ICFE utilice diferentes sistemas operativos, se identificará la mejor manera de mantener sincronizados los diferentes recursos o servicios.

13.17. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS

ICFE debe considerar las siguientes pautas para el uso de programas de utilidad/privilegiados que pueden anular los controles de las aplicaciones, como son:

- Los programas de utilidad se encontrarán restringidos únicamente a los usuarios autorizados.
- Los programas de utilidad deben permitir la identificación, autenticación y autorización, incluyendo el registro del usuario que hace uso de este.
- Los programas utilitarios/privilegiados se encontrarán restringidos para los usuarios finales.
- Los programas utilitarios/privilegiados no deben ser autorizados para usuarios con acceso a aplicaciones donde se requiere segregación de funciones.
- Siempre que se requiera hacer uso de un programa utilitario/privilegiado, el Oficial de Seguridad de la Información debe autorizar el uso de este.
- Se deben eliminar o desinstalar los programas utilitarios/privilegiados que no sean necesarios.
- Se deben mantener y monitorear los registros sobre la utilización de programas utilitarios/privilegiados.

13.18. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

Cumpliendo con las regulaciones y mejores prácticas existentes, ICFE debe contar con un inventario actualizado de software legalmente adquirido y licenciado para cumplir con los objetivos de negocio.

La instalación de cualquier tipo de software en los equipos de cómputo del ICFE, es responsabilidad exclusiva de la oficina de Informática, por tanto, son los únicos autorizados para realizar esta labor.

Ningún tipo de software debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.

Por lo anterior se encuentra prohibido instalar software que no se encuentre en el inventario, y con el fin de evitar incumplimientos a esta política se realiza un monitoreo periódico del software instalado en los equipos de cómputo. Todo software no autorizado será desinstalado por área de Informática.

Frente a los cambios o instalaciones de actualización en los sistemas operativos se debe cumplir con lo siguiente:

- Cualquier cambio que se requiera sobre sistemas operativos debe ser efectuado únicamente por usuarios administradores competentes.
- Utilizar un repositorio de configuración de todos los sistemas operativos y la documentación de estos.
- Archivar todas las versiones anteriores del software, junto con toda la información de parámetros, procedimientos y detalles de configuración como medida de contingencia y durante todo el tiempo que el software lea o procese datos.
- Se deben evaluar los riesgos de utilizar software sin soporte en la infraestructura tecnológica de ICFE, esto incluye software de código abierto.
- La actualización de parches o nuevas versiones de sistemas operativos debe realizarse de forma planificada considerando nuevas funcionalidades y las vulnerabilidades presentes en la versión actual, asegurando que siempre que sea posible se realicen pruebas antes de su instalación en ambiente productivo con el fin de detectar y corregir brechas o debilidades oportunamente.

13.19. SEGURIDAD EN REDES

El área de Informática tendrá bajo su responsabilidad el acceso a los servicios de red tanto internos como externos, así como la implementación de controles en las redes y servicios de red a los cuales se permite el acceso de acuerdo con el tipo y el nivel de clasificación de la información. El área de Informática es responsable de validar la seguridad de los controles de acceso a redes que no administre ICFE sino, que estén a cargo de proveedores o aliados estratégicos.

Para esto se deben considerar los siguientes lineamientos:

a) Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red.

b) Mantener actualizada la información relacionada con Diagramas de red y archivos de configuración, por ejemplo: enrutadores, switches, firewalls entre otros.
c) Mantener registros y realizar monitoreo sobre todas las acciones y actualizaciones relevantes efectuadas sobre las redes y servicios de red.
d) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.
e) Segregar los canales de administración de redes, de otro tráfico de red.
f) Considerar los siguientes controles para salvaguardar la confidencialidad, disponibilidad e integridad de redes internas, públicas o inalámbricas:

- Sistemas de autenticación de la red.
- Listas de control de acceso a los diferentes segmentos de red.
- Hardening de los dispositivos de red.
- Segmentación de la red.
- No deben existir puertos activos sin asignación de servicios que permitan el acceso a la red a personas no autorizadas.
- En el caso de los desarrollos de software internos o externos de ICFE, se debe realizar un análisis sobre los puertos a activar para la operación del aplicativo, esta actividad que debe ser aprobado por el área de Informática o quien este designe.

g) Se debe capacitar y sensibilizar a los colaboradores acerca de la importancia de hacer uso de los controles implementados por ICFE para acceder a las redes y evitar riesgos relacionados con el teletrabajo.

13.20. SEGURIDAD EN LOS SERVICIOS DE RED

Para la seguridad de los servicios de red se deben considerar los siguientes lineamientos:

- Requisitos de autenticación para acceder a las diferentes redes de ICFE como doble factor de autenticación y accesos por VPNs para la consulta de activos críticos de información.
- El área de Informática es el responsable de administrar las redes y los controles tecnológicos que permitan proteger el acceso a redes y servicios de red.
- Se debe almacenar la hora y ubicación del usuario al momento de acceder a la red y realiza seguimiento continuo a actividades no autorizadas.
- ICFE debe implementar controles relacionados con autenticación, cifrado y controles para la conexión a la red.
- Se restringirá el uso de aplicaciones y servicios cuando la compañía lo considere necesario.
- Se debe implementar infraestructura inalámbrica que permita configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas establecidas por defecto.
- Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado entre otros.
- Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a la red Institucional.

Cuando los servicios sean gestionados por proveedores se debe verificar que el tercero cuente con certificaciones que permitan asegurar que se han implementado las medidas de seguridad adecuadas sobre la red de ICFE.

13.21. SEGREGACIÓN DE REDES

La plataforma tecnológica del ICFE que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos, e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet.

La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere. La oficina de Informática es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Se deben garantizar procesos de cifrado y autenticación fuerte en las conexiones VPN con funcionarios que acceden a las bases de datos de servicios productivos.

Cuando un tercero requiera acceder a la red de ICFE, se evaluará la posibilidad de asignarle una VPN de acuerdo con la criticidad de los activos a los que requiere acceso.

13.22. FILTRADO WEB

La navegación en internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

a) Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
b) Publicación, envío o adquisición de material sexualmente explicito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.
c) Publicación o envío de información confidencial hacia afuera del ICFE sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
d) Utilización de otros servicios disponibles a través de internet que permitan establecer conexiones o intercambios no autorizados.
e) Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior debe contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.
f) Promover o mantener asuntos o negocios personales.
g) Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
h) Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte del Instituto.
i) Uso de herramientas de mensajería instantánea no autorizadas por la oficina de informática.

j) Emplear cuentas de correo externas, no corporativas, para el envío o recepción de información institucional.

Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los empleados públicos y terceros autorizados. Así mismo, se pueden inspeccionar, registrar o informar las actividades realizadas durante la navegación.

El uso de internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

13.23. USO DE LA CRIPTOGRAFÍA

Se deben identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento ICFE-P-110 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION, tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la oficina de Informática, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y terceros autorizados.

Los funcionarios, terceros (proveedores y/o contratistas) deben hacer uso apropiado de mecanismos de cifrado para asegurar la integridad, no repudio, confidencialidad y autenticidad de la información crítica de ICFE cuando la información almacenada en medios magnéticos removibles para transporte fuera de las instalaciones físicas de la compañía o enviada a través de correo electrónico o cualquier otro tipo de transferencia digital sea crítica debe transmitirse de forma cifrada, para esto se deben implementar los siguientes lineamientos:

- Definir un procedimiento que permita minimizar los riesgos sobre el uso de técnicas de cifrado y llaves en la compañía.
- Aplicar técnicas de cifrado sobre la información con niveles de clasificación altos.
- Cifrar los datos críticos almacenados (si se requiere) además, de implementar protocolos de comunicación seguros como TLS en las últimas versiones para las comunicaciones.
- Se debe utilizar certificados digitales.
- Las redes inalámbricas que utilice ICFE deben estar configuradas para usar cifrado y autenticación fuerte en sus comunicaciones.
- Para el cifrado, se deben utilizar algoritmos fuertes y probados de proveedores reconocidos.
- Las herramientas de cifrado o firma digital deben ser implementadas por el área de Informática.
- La administración de llaves criptográficas y certificados digitales estará a cargo del área de Informática.

- Documentar procedimientos y gestionar las llaves/certificados con el fin de tener reglas claras frente a creaciones, asignación de accesos, cambios, actualizaciones, almacenamiento, revocación o destrucción de estas.
- Realizar copias de seguridad sobre las llaves/certificados existentes en la compañía.
- Mantener registros de auditoría sobre las actividades ejecutadas con la gestión de llaves/certificados.
- Documentar y mantener registros sobre las fechas de activación y destrucción de las llaves/certificados.
- Efectuar actividades de contención cuando se identifique que las llaves/certificados han sido comprometidos.

13.24. CICLO DE VIDA DE DESARROLLO SEGURO Y REQUISITOS DE SEGURIDAD DE LAS APLICACIONES

Para cualquier ciclo de desarrollo de software incluyendo aplicaciones se deben tener en cuenta los siguientes requisitos dependiendo de la clasificación de la información que va a ser procesada:

- Validación de entradas
- Codificación de salidas
- Administración de autenticación y contraseñas
- Administración de sesiones
- Control de acceso
- Cifrado
- Identificación y seguimiento de transacciones
- Manejo de errores y logs
- Protección de datos
- Seguridad en las comunicaciones
- Configuración de los sistemas
- Seguridad de las bases de datos
- Manejo de archivos
- Manejo de memoria
- Prácticas generales para la codificación
- Practicas contra ataques maliciosos o interrupciones no intencionales

Con el fin de asegurar la implementación de ciclos de desarrollo seguro de software ICFE definirá como requisitos específicos de acuerdo con el tipo de software a desarrollar; entre los requisitos considerados se encuentran:

- Enmarcar el ciclo de desarrollo de software en prácticas, estándares y marcos de referencia que permitan mejorar de forma continua la madurez del ciclo de desarrollo y la postura de seguridad del software, entre los ejemplos a considerar se encuentran: Framework de BSIMM, OWASP SAMM, NIST SSDF, Microsoft SDL y el estándar de verificación de seguridad en aplicaciones de OWASP.
- ICFE establecerá un documento de desarrollo seguro donde se relacionan todas las buenas prácticas y recomendaciones de los marcos de referencia anteriormente relacionados.

- Definir, formalizar y verificar el uso de una metodología de desarrollo seguro para todas las etapas de construcción del software: desarrollo / implementación / adquisición de software.
- En caso de tercerizar los desarrollos ICFE debe garantizar que el proveedor cuente con metodología y documentación de desarrollo seguro.
- Considerar los requisitos de seguridad desde la fase de definición de especificaciones y diseño.
- Establecer puntos de control de seguridad en proyectos.
- Definir pruebas de sistemas y seguridad que considere regresión, escaneo de código y pruebas de penetración.
- Mantener ambientes separados para desarrollo, pruebas y producción y definir los controles requeridos para el aseguramiento de estos.
- Asegurar la utilización de herramientas o repositorios seguros para la gestión del código fuente, configuración y gestión de versiones.
- Asegurar que todo sistema de información que se desarrolle adquiera o contrate como servicio, se le deben aplicar gestión de vulnerabilidades, parches y cambios, así como prácticas de desarrollo seguro.
- Los roles relacionados con el ciclo de desarrollo de software deben contar con conocimientos y habilidades en desarrollo seguro o recibir formación y capacitación.
- La formación o capacitación en desarrollo seguro de software debe realizarse de forma periódica considerando los ciclos de capacitaciones en aspectos de seguridad que realice ICFE.
- Cumplir con los requisitos legales donde se generan, completan, procesan o almacenan las operaciones o transacciones ejecutadas por ICFE.
- Establecer lineamientos para proteger información personal almacenada, en tránsito o en reposo.
- Gestionar los requisitos de licenciamiento para garantizar soluciones rentables y evitar futuros problemas de licencia.
- Realizar una evaluación de riesgos para determinar los requisitos de seguridad de la aplicación cuando se trate de un desarrollo interno o una adquisición.
- Implementar controles de entrada, salida y autorización (validaciones de integridad, double check, integraciones).
- Restricciones en los campos de texto libre ya que pueden conducir al almacenamiento no controlado de datos confidenciales, por ejemplo, datos personales.
- Registrar, almacenar y realizar seguimiento a transacciones.
- El ICFE proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.
- Periódicamente se debe verificar las versiones instaladas tanto en ambiente de pruebas como en producción y se confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de cada institución y entidad del sector.
- Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

- No se permite la copia de Información Ultrasecreta, Reservada, Confidencial, Restringida o Exclusiva, desde el ambiente de producción al ambiente de pruebas; en caso de ser estrictamente necesario, la copia debe contar con las respectivas autorizaciones y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y que se elimine de forma segura después de su uso.
- El paso de software, de un ambiente a otro, debe ser controlado y gestionado de acuerdo con lo definido en el procedimiento ICFE-P-157 CONTROL DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN.

13.25. ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERÍA

ICFE debe establecer y aplicar seguridad en todas las capas de arquitectura (negocios, datos, aplicaciones y tecnología), con el fin de identificar riesgos y mantener diseños seguros frente a amenazas conocidas, para esto contemplará la viabilidad de realizar las siguientes actividades:

a) Analizar los controles de seguridad y verificar su capacidad para prevenir, detectar o responder ante eventos de seguridad y proteger los sistemas de información y la información contra las amenazas identificadas.

b) Evaluar los controles específicos requeridos por procesos de negocio, así como dónde y cómo deben ser aplicados.

c) Asegurar la existencia de controles manuales y automatizados que generen cubrimiento de las brechas identificadas.

d) Los principios de ingeniería deben tener en cuenta:

- La necesidad de integrarse con una arquitectura de seguridad.
- Infraestructura de seguridad técnica.
- La capacidad de la compañía para desarrollar y soportar la tecnología elegida.
- Costo y tiempo de cumplir con los requisitos de seguridad.
- Buenas prácticas actuales.

e) Utilizar principios de arquitectura de seguridad que consideren: “Seguridad por diseño”, “defensa en profundidad”, “Seguridad por defecto”, “denegación predeterminada”, “privilegio mínimo”, entre otros.

f) Identificar oportunamente vulnerabilidades durante la etapa de diseño de los sistemas.

g) Documentar e identificar los controles que no mitigan suficientemente los riesgos de seguridad.

h) Establecer los controles de seguridad técnicos y no técnicos considerando esquemas de autenticación, gestión de sesiones, validación de entradas y salidas,

esquemas de cifrado, manejo de registros y errores, configuraciones, sanitización de datos y criptografía.

i) Implementar hardening sobre productos o servicios (cuando aplique).

j) Implementar principios de zero trust, como son:

- No depender de únicamente de los controles de seguridad de la red.
- Emplear enfoques de “Nunca confiar y siempre verificar”, esto para el acceso a los sistemas de información.
- Garantizar que las comunicaciones entre sistemas estén cifradas de extremo a extremo.
- Utilizar mecanismos de autenticación seguros y aprobados por el oficial de seguridad, incluyendo autenticación fuerte que considere: la identidad del usuario, datos sobre el dispositivo de punto final, clasificación de los datos entre otros aspectos y la respectiva generación de logs para el monitoreo y detección del mal uso de cuentas.
- Aplicar el principio de mínimo privilegio para las cuentas de aplicaciones, componentes, servicios e infraestructura.

k) Seleccionar sistemas operativos para las aplicaciones, contenedores, librerías y lenguajes de programación según las definiciones establecidas por el encargado de la arquitectura empresarial y las líneas base de seguridad.

l) Elaborar el modelado de amenazas durante el diseño del software y ante cambios representativos con el fin de identificar riesgos y contramedidas.

m) Verificar que los niveles de protección contemplen:

- Cifrado
- Comprobación de Integridad
- Retención
- Segregación

13.26. CODIFICACIÓN SEGURA

ICFE debe implementar principios de codificación segura que deben aplicarse sin excepción por los desarrolladores (internos o terceros) con el fin de reducir posibles vulnerabilidades en la construcción del software.

13.27. PRUEBA DE SEGURIDAD EN EL DESARROLLO Y ACEPTACIÓN

ICFE establecerá que las nuevas versiones de software o actualizaciones deben probarse y verificarse de forma detallada, las pruebas ejecutadas deben realizarse de forma integral, considerando pruebas de seguridad y pruebas por componentes, para esto se deben tener en cuenta las siguientes actividades:

- Realizar pruebas sobre el software considerando el plan de pruebas de seguridad a funciones de autenticación, restricción de acceso y criptografía, definidas en la fase

de arquitectura y diseño y con los respectivos soportes o evidencias de los resultados de estas.
- Realizar pruebas sobre la implementación de elementos de codificación segura.
- Realizar evaluaciones de vulnerabilidades independientes.
- Realizar evaluación de código dinámico (DAST).
- Realizar pruebas de penetración para identificar códigos o diseños inseguros.
- Realizar pruebas que permitan validar el aseguramiento de la infraestructura y servicios de cloud utilizados en el desarrollo.
- Usar las herramientas tecnológicas aprobadas por ICFE.
- El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo.
- Garantizar que las pruebas se ejecuten en un ambiente diferente a producción.
- Los planes de pruebas deben considerar: actividades que detallen el objetivo de la prueba y los criterios de aceptación de esta.
- Las pruebas internas deben ser desarrolladas inicialmente por el equipo de desarrollo y luego se deben realizar pruebas independientes para comprobar su funcionalidad (QA).

13.28. DESARROLLO TERCERIZADO

Cuando se tercerizan los servicios de desarrollo de software, ICFE comunicará y acordará los requisitos de seguridad y expectativas al tercero, del mismo modo realizará monitoreo y revisará las actividades ejecutadas por el proveedor de servicios, para esto se deben tener en cuenta las siguientes actividades:

a) Los terceros que realicen desarrollos de software, sin importar el esquema de contratación que se aplique, deben dar cumplimiento a lo especificado en el numeral “Ciclo de vida de desarrollo seguro y requisitos de seguridad de la aplicación” y los lineamientos generales establecidos en la presente política.

b) Establecer acuerdos de licencia, propiedad de código y derechos de propiedad intelectual relacionados con el software subcontratado.

c) Los terceros deben aportar los soportes solicitados por ICFE definidos en el contrato, durante el seguimiento a la prestación del servicio o entrega de productos (software).

d) Se deben identificar y gestionar las amenazas y riesgos relacionados con desarrollos subcontratados.

e) Los terceros se comprometen a realizar por cuenta propia pruebas de seguridad sobre el código fuente y las aplicaciones desarrolladas, así como implementar prácticas de desarrollo seguro.

f) Los terceros deben suministrar evidencia de las pruebas ejecutadas donde se comprueben los niveles alcanzados en seguridad y funcionalidad.

g) Los terceros declaran que cumplen con los requisitos de derechos autor respecto al uso de código fuente, de forma tal que no utilicen código de fuentes no autorizadas.

h) Los terceros deben ejecutar pruebas para asegurar que el software se encuentra libre de vulnerabilidades y software malicioso, estás pruebas deben realizarse antes de la entrega del software.

i) Se deben establecer en el contrato con el tercero, las garantías que aseguren el buen funcionamiento del software y clausulas sobre el acceso y disponibilidad de las fuentes en el caso de que el tercero cese sus operaciones.

j) Se debe establecer en el contrato con el tercero, clausulas relacionadas con:
   - El derecho a auditar procesos y controles de desarrollo.
   - Derechos de autor.
   - Propiedad intelectual sobre el software.
   - Confidencialidad de la información.
   - Habeas Data.

k) Se deben establecer los requisitos de seguridad para el entorno de desarrollo, así como validar la seguridad de librerías, funciones, y/o módulos utilizados, evitando el uso de aquellos elementos que puedan implicar vulnerabilidades en el software.

l) Se debe revisar periódicamente el cumplimiento de los requisitos de seguridad en los desarrollos subcontratados.

m) Para cada uno de los desarrollos subcontratados, se debe tener en cuenta la normatividad aplicable como por ejemplo la ley de protección de datos personales.

13.29. SEPARACIÓN DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

En caso de aplicar, se deben mantener tres ambientes independientes para las soluciones tecnológicas (Desarrollo de software, pruebas y producción). El personal que realiza funciones asociadas a un ambiente específico (desarrollo, pruebas y producción) debe contar con perfiles de acceso que limiten sus actividades exclusivamente al ambiente en el que trabajan, en este orden, el personal de desarrollo no debe tener permisos de modificación al ambiente de pruebas y por ningún motivo al ambiente de producción, cumpliendo con los siguientes lineamientos:

a) Separar lógicamente los ambientes de desarrollo y producción.

b) Definir, documentar e implementar reglas para desplegar el software desde el ambiente de desarrollo hasta el ambiente de producción.

c) Probar los cambios en un ambiente de pruebas previo a su implementación en producción.

d) No utilizar información confidencial en entornos de desarrollo y pruebas.

e) Sólo el ambiente de desarrollo dispondrá de herramientas y utilitarios de desarrollo. Éstas estarán restringidas en los otros ambientes.

f) El ambiente de pruebas debe ser una réplica del de producción en lo que respecta a programas y condiciones de ejecución y el sistema de control de acceso debe ser diferente e independiente.

g) ICFE podrá utilizar datos de producción en el ambiente de pruebas siempre y cuando estos se encuentren enmascarados. El uso de estos datos debe ser autorizado por el oficial de seguridad de la información.
h) No realizar pruebas en entornos de producción, solo en circunstancias en donde se cuente con la aprobación del oficial de seguridad de la información.

i) Los ambientes de desarrollo y pruebas deben implementar los siguientes controles:

- Aplicación de parches y actualización de todas las herramientas de desarrollo, integración y pruebas.
- Configuración segura de sistemas y software.
- Controles de acceso.
- Aprobación y seguimiento a cambios y al código almacenado.
- Monitoreo de los ambientes.
- Evaluar la ejecución de copias de seguridad sobre los diferentes entornos.
- Segregación de funciones y derechos de acceso.

j) Una sola persona no debe contar con privilegios para realizar cambios en los diferentes ambientes, cuando existan situaciones excepcionales estás debe ser registradas y monitoreadas mediante logs de auditoría.

k) El ambiente del sistema de prueba debe emular el ambiente de producción, lo más estrechamente posible.

13.30. GESTIÓN DE CAMBIOS

Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la oficina de Informática, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deben estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento ICFE-P-157 CONTROL DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN. Dicha definición debe ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

Hay que asegurar que toda la documentación operativa sea actualizada luego de la implementación de cambios en ambiente productivo, para esto se deben tener en cuenta los planes de respaldo de la información y de continuidad tecnológica.

13.31. INFORMACIÓN DE LAS PRUEBAS

La información utilizada para la ejecución de pruebas debe seleccionarse para garantizar la efectividad de los resultados de las pruebas realizadas, teniendo en cuenta que los datos de identificación personal deben ser enmascarados para los ambientes de desarrollo y pruebas, para esto se han definido e implementado los siguientes lineamientos:

- Se aplican procedimientos de control de acceso para los ambientes de pruebas y operativos.
- ICFE podrá utilizar datos de producción en el ambiente de pruebas siempre y cuando estos se encuentren enmascarados o cifrados. El uso de estos datos debe ser autorizado por el oficial de seguridad de la información.
- Se mantienen registros del uso de información proveniente de ambientes productivos, como insumo para auditorias.
- Se elimina la información utilizada en ambientes de pruebas, inmediatamente después de finalizada la actividad (Cuando aplique).
- Se almacena la información de forma segura con el fin de evitar la manipulación de esta.

13.32. PROTECCIÓN DE SISTEMAS DE INFORMACIÓN DURANTE PRUEBAS DE AUDITORÍA QUE INVOLUCREN TI

Las auditorías que se programen en ICFE y que involucren la evaluación de infraestructura o sistemas de información, deben planificarse con los lideres de los procesos y cumplir con los siguientes lineamientos:

- Contar con perfiles especiales para ser usados por la función de auditoría. Cuando se requiera, los auditores tendrán privilegios para consultar la información del negocio de acuerdo con su clasificación y no podrán realizar cambios sobre la misma. En caso de no poder otorgar los permisos, la prueba debe ser realizada en compañía de un administrador experimentado que cuente con los derechos de acceso necesarios.
- El alcance de la auditoría debe ser comunicado al personal involucrado.
- Antes de permitir el acceso, se debe verificar el cumplimiento de la línea base de seguridad del equipo proporcionado al equipo auditor, como: antivirus y parchado.
- Cuando se requieran privilegios diferentes a lectura, el acceso se otorgará únicamente sobre copias aisladas de archivos del sistema, eliminándolos cuando se complete la auditoría.
- La utilización de las herramientas de auditoría debe ser acordada entre las partes.
- La ejecución de pruebas de auditoría que puedan afectar la disponibilidad de los sistemas debe ser ejecutada fuera del horario laboral, en caso de ser requerida la ejecución dentro del horario laboral, estas deben ser aprobadas por el Líder del producto.
- Los auditores deben firmar acuerdos de confidencialidad antes de la ejecución del proceso auditor.
- Los accesos otorgados a auditoría de deben ser registrados, supervisados y deshabilitados una vez finalice el proceso de auditoría.

12. REGISTROS Y DOCUMENTOS ASOCIADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
ICFE-P-110-F-01	FORMATO DE INVENTARIOS DE ACTIVOS DE INFORMACIÓN
ICFE-M-10 F-01	FORMATO ACUERDO DE CONFIDENCIALIDAD
ICFE-P-141 F-01	FORMATO AUTORIZACION INGRESO/SALIDA – EQUIPOS INSTITUCIONALES
ICFE-P-141 F-02	FORMATO AUTORIZACION INGRESO/SALIDA – EQUIPOS ENTIDADES EXTERNAS
ICFE-P-131 F-01	FORMATO REPORTE INCIDENTES DE SEGURIDAD
ICFE-P-130	PROCEDIMIENTO PARA LA GESTION DE INCIDENTES DE SEGURIDAD
ICFE-P-110	PROCEDIMIENTO DE INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION
ICFE-P-157	CONTROL DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN
ICFE-P-158	GESTION DE LA CAPACIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN
ICFE-P-156	PROCEDIMIENTO DE GESTION DE LAS VULNERABILIDADES TECNICAS
ICFE-P-37	GENERACIÓN DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN
ICFE-P-159	PROCEDIMIENTO GESTION DE USUARIOS Y CONTRASEÑAS

14. REGISTRO DE MODIFICACIONES (espacio exclusivo para calidad)

VERSIÓN	FECHA MODIFICACIÓN	NUMERAL MODIFICADO	NATURALEZA DEL CAMBIO
04	13-06-2016	Todo	Se actualiza el documento
05	23-06-2024	Todo	Se actualiza el documento según la actualización de las normas.
06	23-12-2024	Todo	Se actualiza el documento según las necesidades del negocio.