Hacienda
Secretaría de Hacienda y Crédito Público

CONDUSEF

COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Octubre 2025

ÍNDICE

DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La Dirección de Planeación y Finanzas con la participación de la Dirección de Tecnologías de la Información y Comunicaciones, en ejercicio de las atribuciones que les son conferidas en los artículos 14, fracción III; 37, fracción XIX; y 39, fracciones I, IV, VII y VIII respectivamente, del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, se dieron a la tarea de actualizar las **"Políticas de Seguridad de la Información".**

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), tiene la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad; de este modo, la CONDUSEF no discrimina por razón alguna o condición, incluyendo aquellas que se refieran al origen étnico o nacional, género, edad, discapacidad, condición social, condiciones de salud, religión, preferencia sexual, estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto vulnerar los derechos y libertades de las personas.

La CONDUSEF rechaza las conductas que, de forma directa o indirecta, intencional o no, propicien un trato de distinción, exclusión o restricción que tengan como resultado afectar el reconocimiento, goce o ejercicio de uno o más derechos humanos, por lo que está comprometida a respetar los principios democráticos y los derechos humanos de las personas en general.

El lenguaje empleado en este instrumento no busca generar ninguna discriminación, ni marcar diferencias entre mujeres y hombres, y las referencias o alusiones a los sujetos, representan siempre a hombres y mujeres.

I. ÁMBITO DE APLICACIÓN, RESPONSABLES Y OBLIGACIONES

Las disposiciones contenidas en las presentes Políticas serán de aplicación obligatoria para todos los Usuarios de bienes, servicios informáticos y cualquier activo de TIC, y para los servidores públicos adscritos a la Dirección de Tecnologías de la Información y Comunicaciones, en el ámbito de su competencia.

Los titulares de las áreas involucradas serán responsables de su observancia y difusión entre el personal bajo su mando, así como de llevar a cabo revisiones periódicas, para que su contenido corresponda a su operación y normatividad vigentes, a fin de que se constituya como una herramienta de trabajo eficaz.

La Dirección de Planeación y Finanzas, será la responsable de la actualización y mejoramiento de estas Políticas, con base en las propuestas y requerimientos que formulen las áreas responsables de los procedimientos.

Su difusión en la CONDURED se realizará a través del responsable de administrar y operar la Normateca Interna.

II. MARCO JURÍDICO – ADMINISTRATIVO

Ordenamientos de Tipo Legislativo

- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- Ley de Protección y Defensa al Usuario de Servicios Financieros.
- Ley Federal de Austeridad Republicana.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Responsabilidades Administrativas.
- Ley Orgánica de la Administración Pública Federal.
- Ley para Regular las Instituciones de Tecnología Financiera.

Ordenamientos de Alcance General

- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el Gobierno Digital, las Tecnologías de la Información y Comunicación, y la Seguridad de la Información en la Administración Pública Federal.
- Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.
- Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.

Ordenamientos Normativos Internos

- Manual de Organización General de la CONDUSEF.

III. DEFINICIONES Y ACRÓNIMOS

Para los efectos de estas Políticas, además de las definiciones previstas en el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el Gobierno Digital, las Tecnologías de la Información y Comunicación, y la Seguridad de la Información en la Administración Pública Federal, se entenderá por:

Activo de Información	A la información y medio que la contiene, que por su importancia y el valor que representa para la CONDUSEF, debe de ser protegido para mantener su confidencialidad, integridad y disponibilidad, acorde al valor que se le otorgue.
Activo de TIC	A los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
Acuerdo	Al Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
Acuerdo de Confidencialidad	Al referido en el artículo 2°, fracción III del Acuerdo.
Administrador de Usuarios	A la persona responsable de agregar, administrar y eliminar Usuarios de un sistema.
Amenaza	A la referida en el artículo 2°, fracción V del Acuerdo.
Aplicativo informático	Al programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
Aviso de Privacidad	Al Documento que se encuentra a disposición del titular de los datos personales de forma física, electrónica o en cualquier formato generado por el responsable, con el objeto de informarle los propósitos del tratamiento de los mismos a partir del momento en el cual se recaben sus datos personales.

Borrado seguro	Al referido en el artículo 2°, fracción IX del Acuerdo.
Centro de Datos	Al referido en el artículo 2°, fracción X del Acuerdo.
Comisión Nacional/ CONDUSEF	A la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.
Confidencialidad	A la característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.
Disponibilidad	A la característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.
DTIC	A la Dirección de Tecnologías de la Información y Comunicaciones.
Esquema de Gobierno de Seguridad	A la forma de organización que busca preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados.
Evento de Seguridad	Al suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.
Incidente de Seguridad	A la afectación o interrupción de los Activos de TIC, a las infraestructuras críticas, así como a los Activos de Información de la CONDUSEF, incluido el acceso no autorizado o programado a éstos.
Integridad	A la acción de mantener la exactitud y corrección de la información y sus métodos de proceso.
LGPDPPSO	A la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

MGSI	Al Marco de Gestión de Seguridad de la Información.
Plan de Contingencia	Al instrumento de gestión para el manejo de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y desempeño.
Plan de Continuidad del Negocio (BCP)	Al proceso de desarrollar arreglos previos y procedimientos que sirven como capacitación para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción.
Plan de Recuperación de Desastres (DRP)	Al proceso que determina cómo realizar una copia de seguridad de los datos.
Política	A la intención e instrucción global en la manera que formalmente ha sido expresada por la dirección de la Institución.
Riesgo	Al referido en el artículo 2°, fracción XL del Acuerdo.
RSI	Al Responsable de Seguridad de la Información.
Seguridad de la Información	A la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Seguridad Informática	A la protección de la información con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas.
Tecnologías de la Información y Comunicación	A las referidas en el artículo 2°, fracción XLVI del Acuerdo.
Terceros	A la persona o entidad que está reconocida como independiente de las partes implicadas para el asunto en cuestión.
Usuario	A los servidores públicos o aquellos Terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de Tecnologías de la Información y Comunicaciones.

IV. OBJETIVO

Establecer las directrices que deberán observar los servidores públicos y Terceros interesados, con el fin de proteger y garantizar la Confidencialidad, Integridad y Disponibilidad de los activos de información de la Comisión Nacional, contribuyendo así al cumplimiento de sus funciones institucionales en un entorno seguro y controlado.

V. PROCEDIMIENTO Y APLICACIÓN DE LAS POLÍTICAS

1. POLÍTICA DE ORGANIZACIÓN INTERNA DE SEGURIDAD DE LA INFORMACIÓN

A. Gestión de la Seguridad de la Información

A.1. La DTIC, será la responsable de alinear las acciones en materia de seguridad con los requerimientos normativos y estratégicos de la CONDUSEF.

A.2. El Titular de la DTIC como RSI, definirá, implementará, controlará y gestionará políticas, procedimientos y mecanismos para proteger la confidencialidad, integridad y disponibilidad de la información institucional.

B. Estructura Organizativa de la Seguridad de la Información

B.1. La CONDUSEF ha establecido un Esquema de Gobierno de Seguridad de la Información, como marco organizacional para gestionar eficazmente todas las actividades relacionadas con la seguridad de la información.

B.2. Este esquema se basa en roles definidos que respaldan las funciones necesarias para su adecuada administración, y se estructura en tres niveles jerárquicos: estratégico, táctico y operativo. El nivel estratégico establece la visión, políticas y recursos; el táctico coordina la implementación de controles y planes operativos; y el operativo ejecuta las acciones y aplica los controles definidos, asegurando la protección de la información institucional con una clara segregación de funciones.

A continuación, se detalla la estructura del Esquema de Gobierno de Seguridad de la Información **(Fig. 1.)**, de acuerdo con los niveles de responsabilidad.

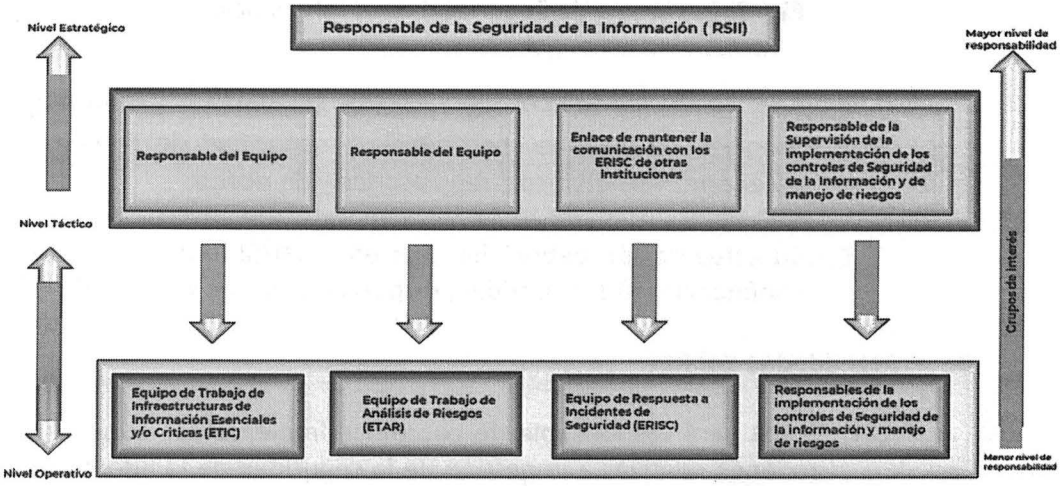
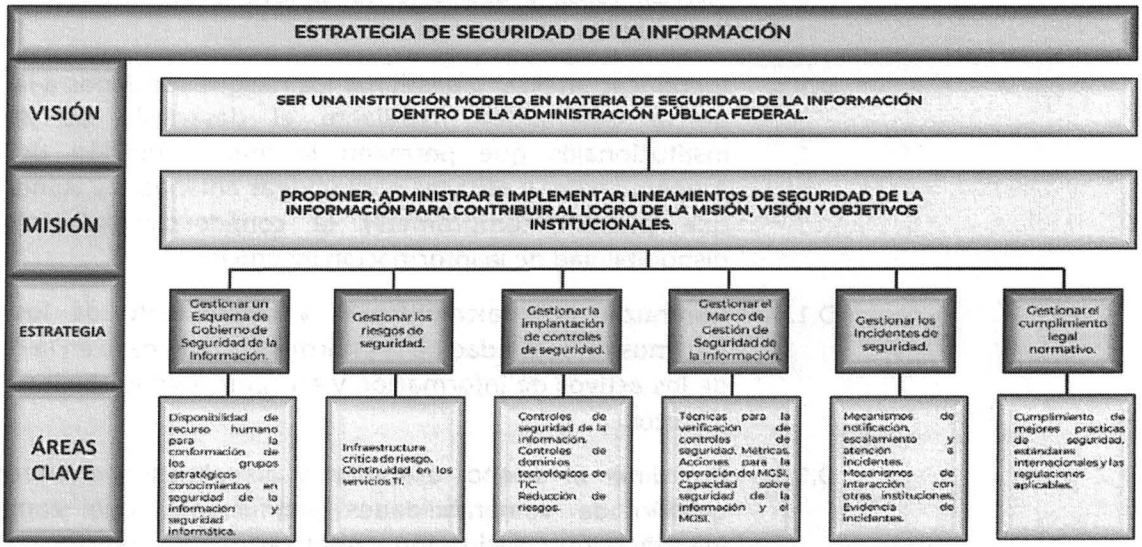


Fig. 1. "Esquema de Gobierno de Seguridad de la Información"

C. Estrategia de Seguridad de la Información

C.1. La Estrategia de Seguridad de la Información será definida con base en los objetivos institucionales de la CONDUSEF, asegurando que su implementación apoye el cumplimiento de la misión y visión organizacional



como se describe a continuación.

Fig. 2. Estrategia de Seguridad de la Información

C.2. Esta estrategia deberá ser revisada anualmente por el RSI, con el fin de asegurar su vigencia, pertinencia y capacidad de respuesta ante nuevos escenarios tecnológicos, regulatorios y de riesgo.

C.3. Su actualización deberá basarse en el MGSI, enfocándose en garantizar la confidencialidad, integridad, disponibilidad y no repudio de la información.

D. Actividades del RSI

D.1. El RSI será responsable de coordinar, implementar, supervisar y evaluar las acciones relativas a la gestión de la seguridad de la información dentro de la institución, en cumplimiento con las disposiciones establecidas en el marco normativo vigente. Las funciones que deberá desempeñar incluyen:

D.1.1. El RSI deberá diseñar, coordinar y mantener el MGSI institucional, asegurando su alineación con la política general de seguridad de la información, así como con los objetivos estratégicos, regulatorios, organizacionales, operativos y de cultura de seguridad de la información de la Institución.

D.1.2. Mantener y fortalecer los vínculos institucionales con grupos de interés, foros y asociaciones especializadas en seguridad de la información.

D.1.3. Identificar, analizar y gestionar los riesgos asociados a la seguridad de la información, mediante el desarrollo de diagnósticos institucionales que permitan la implementación de controles proporcionales y eficaces para mitigar amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

D.1.4. Garantizar la implementación y seguimiento de los controles mínimos de seguridad de la información, con base en la clasificación de los activos de información y en cumplimiento de los estándares técnicos

D.1.5. Coordinar el diseño, ejecución y actualización del programa de gestión de vulnerabilidades institucional, que contemple su identificación, evaluación, priorización y atención, incluyendo aquellas detectadas a través de fuentes externas especializadas.

D.1.6. Diseñar, establecer y mantener el protocolo institucional de respuesta ante incidentes de seguridad de la información, que incluya la conformación del Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), la definición de roles, actividades de preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.

D.1.7. Coordinar la formulación y mantenimiento del plan de continuidad de operaciones y del plan de recuperación ante desastres en materia de TIC, garantizando su integración con los servicios críticos de la institución y la protección de los activos de información.

D.1.8. Promover la formación y fortalecimiento de la cultura institucional de seguridad de la información, mediante el diseño e implementación de programas de capacitación, sensibilización y concientización dirigidos a todas las personas servidoras públicas de la Institución.

D.1.9. Establecer y coordinar grupos de trabajo institucionales para la definición, implementación, operación y evaluación del MGSI, asegurando que sus objetivos, actividades y roles sean formalmente documentados.

D.1.10. Participar en los procesos de planeación, justificación y contratación de bienes y servicios relacionados con la seguridad de la información, asegurando que las adquisiciones cumplan con la normatividad vigente y contribuyan a la implementación efectiva del MGSI.

D.2. Las actividades de revisión, mantenimiento o mejora de los activos tecnológicos y controles de seguridad no deberán afectar la operación institucional. En caso de que se requiera suspender temporalmente servicios o procesos, dichas actividades deberán ser planificadas con anticipación y comunicadas oportunamente al personal involucrado.

E. Acuerdos de Confidencialidad

E.1. Se deberán establecer mecanismos de borrado seguro de archivos y documentos institucionales, así como Acuerdos de Confidencialidad o no divulgación de la Información con todos los Usuarios (servidores públicos y Terceros), que tengan acceso a la información de la CONDUSEF, así como comprometerse a cumplir con lo establecido en el presente documento.

E.2. Los Acuerdos de Confidencialidad o no divulgación, deberán ser identificados y revisados regularmente, asegurando que se cumplan las necesidades de protección de la información de la CONDUSEF.

E.3. Los prestadores de servicios por honorarios, honorarios asimilados a salarios y los servidores públicos con la CONDUSEF deberán contener Cláusulas de Confidencialidad.

F. Contacto con las Autoridades

F.1. El RSI deberá tener actualizado el documento que integre la información correspondiente a las autoridades competentes en materia de seguridad (policías, bomberos, protección civil, órganos reguladores, etc.).

F.2. El responsable de la seguridad física definirá el procedimiento que especifique cuándo y con qué autoridades se deberá contactar, y la manera adecuada de cómo hacerlo, ante la presencia de un Incidente de Seguridad en la CONDUSEF.

F.3. El RSI revisará periódicamente el procedimiento y el documento con la información de contacto de las autoridades, para verificar que los datos se mantengan actualizados.

G. Contacto con Organizaciones de Especial Interés

G.1. Deberán mantenerse contactos adecuados con grupos de interés, foros y asociaciones especializados en seguridad.

G.2. La participación de estos grupos deberá:

G.2.1. Mejorar el conocimiento sobre las principales prácticas en materia de Seguridad de la Información y mantenerse actualizado.

G.2.2. Asegurar que la comprensión del entorno de Seguridad de la Información es actual y correcto.

G.2.3. Recibir avisos tempranos de alertas, asesoramiento y parches correspondientes a los ataques y vulnerabilidades.

G.2.4. Obtener acceso al asesoramiento especializado en Seguridad de la Información.

G.2.5. Compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades.

G.2.6. Proporcionar puntos de enlace relacionados con Incidentes de Seguridad de la Información.

G.3. Podrán establecerse acuerdos de intercambio de información para mejorar la cooperación y la coordinación en la parte de seguridad, a fin de proteger la información, siempre y cuando se cumplan los Acuerdos de Confidencialidad en la Seguridad de la Información y Protección de Datos Personales.

H. Revisión Independiente de la Seguridad de la Información

H.1. El RSI, considerará revisiones independientes para llevar a cabo la verificación de la Seguridad de la Información.

H.2. La revisión de Seguridad de la Información deberá considerar como mínimo lo siguiente:

H.2.1. Identificar la implementación y apego a los controles definidos para proteger la información.

H.2.2. Detectar la ausencia de controles y con ello, la existencia de posibles riesgos de seguridad.

H.2.3. Identificar la causa u origen de un evento de seguridad y/o incidentes de seguridad.

H.2.4. Proporcionar las recomendaciones pertinentes.

H.3. Las actividades desarrolladas por la CONDUSEF no se verán afectadas mientras el RSI efectúa la revisión y el mantenimiento de los activos de TI. En caso de ser necesario suspender actividades para llevar a cabo el análisis correspondiente a la Seguridad de la Información, éstas deberán planificarse con antelación y se informará al personal para evitar complicaciones durante la jornada laboral.

H.4. Las revisiones independientes deberán realizarse a intervalos, planificados por el RSI, o siempre que se produzcan cambios significativos en la Seguridad de la Información.

I. Tratamiento de la Seguridad en Contratos con Terceros

I.1. Para efectos de la elaboración y suscripción de contratos o convenios que se efectúen con Terceros, dependiendo de la naturaleza del proyecto, se deberán tener en consideración los siguientes puntos:

I.1.1. Cumplimiento de las Políticas de Seguridad de la Información.

I.1.2. Protección de los Activos de Información.

I.1.3. Descripción y alcance de los servicios contratados.

I.1.4. Nivel de servicio esperado y niveles de servicio aceptables (umbral de desviación).

I.1.5. Evaluación y autorización para la rotación de los servidores públicos cuando sea necesario.

I.1.6. Cláusulas de confidencialidad y protección de datos personales.

I.1.7. Obligaciones de las partes que suscriben el contrato.

I.1.8. Existencia de Derechos de Propiedad Intelectual tales como:

a. Autorización de Uso o Licenciamiento.
b. Cesión de Derechos.
c. Derecho a Actualizaciones.

I.1.9. Acuerdos de control de accesos que contemplen:

a. Métodos de acceso permitidos.
b. El control y uso de identificadores únicos de Usuario y contraseñas.
c. Procedimiento de autorización de accesos y privilegios de Usuarios.

I.1.10. Requerimiento para mantener actualizada permanentemente, una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus obligaciones, derechos y privilegios con respecto a dicho uso.

I.1.11. Definición de criterios de desempeño comprobables de monitoreo y de presentación de informes.

I.1.12. Actividades de auditoría de responsabilidades contractuales o surgidas del acuerdo con Terceros

I.1.13. Establecimiento de un proceso para la resolución de problemas y, en caso de no corresponder, disposiciones con relación a situaciones de contingencia.

I.1.14. Responsabilidades relativas a la instalación, configuración, puesta a punto y al mantenimiento de hardware y software.

I.1.15. Proceso claro y detallado de administración de cambios.

I.1.16. Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

I.1.17. Planes de entrenamiento y capacitación de Usuarios y administradores en materia de seguridad.

I.1.18. Controles que garanticen la protección contra software malicioso.

I.1.19. Elaboración y presentación de informes, notificación, investigación y estudio de incidentes y violaciones relativos a la seguridad.

I.1.20. Relación entre Terceros y subcontratistas.

I.1.21. Donde haya necesidad de permitir el acceso a Terceros a los dispositivos de tratamiento de información de la CONDUSEF, deberá llevarse a cabo una evaluación de riesgo para conceder los privilegios adecuados de acción y, en su caso, las firmas físicas o electrónicas de los controles específicos.

I.1.22. El acceso a Terceros deberá darse cuando se hayan implantado los controles, y cuando sea posible tener firmado un contrato que defina los términos y condiciones para la conexión a los activos de la CONDUSEF.

I.1.23. La CONDUSEF deberá asegurarse que el Tercero conoce sus obligaciones y acepta las responsabilidades y limitaciones que lleva implícito el acceso, procesado, comunicación o gestión de la información y de los recursos de tratamiento de Seguridad de la Información.

I.1.24. Manejo de información y los activos al finalizar el contrato o acuerdo (o momento específico convenido durante la vigencia del mismo), para garantizar la recuperación o destrucción de la información.

I.1.25. Borrado seguro de la información y resguardo de la información compartida o la que se tuvo acceso o almacenamiento y obtención de evidencia en términos de la normativa aplicable.

J. Tratamiento de Datos Personales

J.1. Es responsabilidad de la DTIC aplicar los principios que rigen la protección de los datos personales de acuerdo a los términos impuestos por la LGPDPPSO, garantizando los deberes de seguridad y confidencialidad bajo los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad. La obligación adquirida por la DTIC ante los servidores públicos que se desempeñan en el área es:

J.1.1. Aplicar las buenas prácticas en seguridad de la información que avalen la protección de los datos personales.

J.1.2. Contar con el consentimiento de los servidores públicos para el tratamiento de sus datos personales.

J.1.3. Mantener actualizados los datos personales, cuando sean modificados por el titular de los mismos.

J.1.4. Deberá informar al titular a través del aviso de privacidad la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin que pueda tomar decisiones informadas al respecto.

J.1.5. Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas, lícitas y legítimas que motivaron su tratamiento.

J.1.6. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento.

J.1.7. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo solo tratarlos para almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

J.1.8. Suprimir los datos personales, previo bloqueo, cuando haya concluido el tiempo requerido para llevar a cabo las finalidades del tratamiento.

J.1.9. No difundir o compartir con terceros los datos personales del titular, salvo que se cuente con el consentimiento para ello, o bien, por alguna obligación normativa que exija su difusión.

J.1.10. Queda prohibido el tratamiento de datos personales que tenga como efecto la discriminación de sus titulares por su origen étnico o racial, su estado de salud presenta, futuro o pasado, su información genética, sus opiniones políticas, su región o creencias filosóficas o morales o su preferencia sexual.

J.1.11. Mantener medidas de seguridad administrativas, físicas y técnicas con el propósito de proteger los datos personales contra daño, perdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

2. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

A. Compromiso de Confidencialidad y Manejo Responsable de Datos Personales

A.1. Todo el personal que tenga acceso a información que contenga datos personales deberá firmar una Carta Responsiva de Acceso a la Información y Datos Personales, como parte del proceso de alta institucional, esta tiene como finalidad establecer el compromiso de confidencialidad, uso adecuado y protección de dicha información.

A.2. Todos los Usuarios de la CONDUSEF, y cuando sea necesario, los contratistas y Terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas, procedimientos y expectativas de la Comisión Nacional en términos de Seguridad de la Información.

A.3. Se impartirá capacitación a los Usuarios de acuerdo con el rol y responsabilidad que cada uno tendrá a su cargo dentro de la CONDUSEF.

A.4. La capacitación deberá garantizar al Usuario el nivel de conocimiento necesario, para poder actuar ante amenazas en Eventos de Seguridad, a fin de prevenir riesgos y/o poder minimizar el impacto en caso de su materialización.

A.5. La DTIC, deberá asegurarse que todo Usuario con responsabilidades en el MGSI, sea competente para realizar las tareas que le son requeridas.

A.6. La DTIC, deberá asegurarse que todo Usuario esté consciente de la relevancia de las actividades de Seguridad de la Información que tiene a su cargo, así mismo deberá capacitar al Usuario de cómo puede contribuir para mantener la Confidencialidad, Integridad y Disponibilidad de la Información.

B. Tratamiento de Datos Personales

B.1. Las áreas que recaben, usen, almacenen o transmitan datos personales deberán asegurar que dicho tratamiento se realice con base en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

B.2. Deberá garantizarse que los titulares de los datos personales sean informados sobre el tratamiento de su información mediante la difusión clara, accesible y actualizada del Aviso de Privacidad, ya sea en modalidad simplificada, integral o corta, según corresponda, asegurando que este documento esté disponible en los medios físicos o electrónicos por los cuales se recaben o traten los datos.

B.3. Las áreas responsables deberán aplicar las medidas de seguridad necesarias para proteger los datos personales en posesión de la institución, evitando el acceso, uso, divulgación, modificación o destrucción no autorizada.

B.4. Las áreas responsables del desarrollo, operación o mantenimiento de aplicaciones web y móviles que involucren el tratamiento de datos personales deberán implementar controles técnicos y organizacionales para mitigar riesgos, como cifrado de información, autenticación robusta, control de acceso y pruebas de seguridad.

B.5. Establecer un ciclo de vida de los datos en el que se garantice su actualización y eliminación o destrucción conforme a los plazos establecidos en las políticas de protección de datos.

B.6. Se prohíbe el tratamiento de datos personales que tenga como resultado o finalidad la discriminación de los titulares por motivos de origen étnico o racial, estado de salud presente, futuro o pasado, información genética, opiniones políticas, creencias filosóficas o morales, religión o preferencia sexual.

B.7. La DTIC, deberá conservar los registros correspondientes a la capacitación, como:

1) Calendario de Capacitación Anual.
2) Material del Curso.
3) Listas de Asistencias.
4) Evaluaciones del Curso.
5) Constancias.

B.8. Se deberán realizar evaluaciones para identificar los resultados de la capacitación y poder determinar que el Usuario es apto para continuar con las responsabilidades que tiene a su cargo; de lo contrario, debe diseñarse un nuevo Programa de Capacitación hasta lograr su éxito en la transmisión de conocimiento.

B.9. La DTIC, deberá asumir las siguientes responsabilidades:

B.9.1. Comunicar claramente a los Usuarios, las responsabilidades relacionadas a la Seguridad de la Información, antes de darles acceso a información privilegiada y/o confidencial.

B.9.2. Brindarles los recursos para que conozcan las Políticas de Seguridad de la Información.

B.9.3. Disponer de una mesa de ayuda donde el Usuario recibirá el apoyo de los encargados de la SI o soporte técnico y el alcance de las solicitudes abarque los siguientes rubros: sospecha ante un ataque de virus informático en los equipos de cómputo, consulta respecto a las políticas de seguridad de la información que rigen a la CONDUSEF, creación de Usuarios y contraseñas seguros, apoyo en la implementación de una VPN, configuración de cuentas de Usuario, correcto uso del internet y de los navegadores, entre otros.

B.9.4. Motivarlos constantemente para cumplir cabalmente con las Políticas de Seguridad de la Información.

B.9.5. Identificar y reconocer las buenas prácticas en seguridad de la información como:

1) Generación de copias de seguridad
2) Actualización constante
3) Apegarse a las presentes políticas
4) Cumplir las responsabilidades asignadas en materia de SI

B.9.6. Brindar las facilidades para que participen en los programas de concientización relativos a la Seguridad de la Información.

B.10. Los servidores públicos, prestadores de servicios y Terceros, deberán apegarse a las políticas y procedimientos establecidos por la CONDUSEF; así mismo deberán ser conscientes de las responsabilidades que tienen a su cargo, a fin de evitar impactos negativos en la seguridad.

B.11. Se establecerá el proceso de capacitación en materia de Seguridad de la Información como elemento continuo, que garantice el conocimiento y habilidades necesarias del Usuario para procurar la Confidencialidad, Integridad y Disponibilidad de los Activos de Información con los que interactúa para ejercer las actividades necesarias bajo su cargo en la CONDUSEF.

B.12. Los administradores de contratos deben asegurarse que los prestadores de servicios cumplan con lo establecido en las presentes políticas.

3. POLÍTICA DE CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD

A. Criterios generales

A.1. La DTIC ha tenido a bien desarrollar el Programa de Formación, Concientización y Capacitación en materia de Seguridad de la Información, con el propósito de fomentar entre las personas servidoras públicas de la CONDUSEF una cultura de corresponsabilidad, sensibilización e involucramiento activo en la protección de los activos de información institucional.

A.2. Cada Usuario será responsable de la cuenta de Usuario que le sea proporcionada para acceder a la información y a la infraestructura tecnológica de la CONDUSEF. La cuenta es para uso personal e intransferible.

A.3. La cuenta de Usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de Usuario, deberá seguir los Criterios para la Construcción de Contraseñas conforme a lo establecido en las presentes Políticas.

A.4. Los Usuarios serán responsables de todas las actividades realizadas con su cuenta de Usuario, por lo cual, deberán abstenerse de divulgar su identificador a Terceros, así como de utilizar cuentas de Usuarios que no les pertenezcan.

A.5. Los Usuarios, deberán tratar cada contraseña asignada con carácter confidencial.

A.6. Las contraseñas de ninguna manera podrán ser transmitidas por los Usuarios mediante servicios de correo electrónico, instantánea, ni vía telefónica; por lo que su entrega a éstos por la DTIC será:

A.6.1. A través del personal del Departamento encargado de las asignaciones de las contraseñas en la DTIC, quien entregará en persona al Usuario la contraseña de acceso a su equipo de cómputo, obteniendo acuse de recibo por parte del Usuario, o bien, a través del área correspondiente de la asignación de cuentas de Usuario y contraseñas de la DTIC, quien deberá asegurar que un solo responsable, el cual deberá tener el rol de administrador, tenga la

autoridad para la creación de accesos para cualquiera de los servicios y/o sistemas que operan dentro de la CONDUSEF, quien deberá asegurarse de contar con una persona alterna que conozca el proceso para garantizar la continuidad.

A.7. Será responsabilidad de cada Usuario no mencionar y teclear contraseñas en frente de otros.

A.8. Será responsabilidad de cada Usuario no revelar contraseñas en cuestionarios, reportes o cualquier otro documento que quede a la vista de otra persona.

A.9. Los Usuarios no podrán utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.

A.10. Los Usuarios deberán activar o hacer uso de la opción de recordar contraseña o recordar credenciales de acceso a las aplicaciones.

A.11. No se deberá almacenar las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. El respaldo de las contraseñas deberá quedar en medio impreso, a través de una carta responsiva generada por la DTIC deberá ser única y bajo resguardo.

A.12. Si alguna contraseña es detectada y catalogada como no segura por la DTIC, deberá darse aviso al(los) Usuario(s) para efectuar un cambio inmediato en dicha contraseña.

A.13. Si la DTIC detecta o sospecha que la actividad de una cuenta de Usuario puede comprometer la Integridad y Seguridad de la Información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración del Administrador del Sistema.

A.14. Todas las contraseñas para acceso al Sistema con carácter administrativo deberán ser cambiadas al menos cada 3 meses, para lo cual la DTIC realizará los requerimientos correspondientes.

A.15. Todas las contraseñas para acceso al Sistema de nivel Usuario deberán ser cambiadas al menos cada 3 meses, para lo cual la DTIC realizará los requerimientos correspondientes.

A.16. Cualquier cambio en los roles y responsabilidades de los Usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la CONDUSEF, deberá ser solicitada mediante escrito a la DTIC por el Titular de la Unidad Administrativa de que se trate.

B. Capacitación general

B.1. La DTIC promoverá la inclusión de contenidos de seguridad de la información en las actividades institucionales de capacitación, a fin de que todo el personal cuente con una base mínima de conocimientos en la materia.

B.2. Los contenidos de capacitación general incluirán aspectos como:

- Principios básicos de seguridad digital.
- Buenas prácticas en el uso del correo institucional, contraseñas y navegación segura.
- Procedimientos para respaldo de información y protección de dispositivos.
- Identificación y notificación de eventos sospechosos o incidentes de seguridad.

B.3. La participación del personal de la CONDUSEF en las actividades de capacitación será registrada por la DTIC, y el cumplimiento de esta capacitación formará parte de las responsabilidades funcionales de cada persona usuaria.

C. Sensibilización en Seguridad de la Información

C.1. La DTIC deberá fomentar la cultura de seguridad de la información mediante la difusión regular de contenidos informativos y materiales de sensibilización, accesibles a todo el personal.

C.2. Esta difusión incluirá, como mínimo, temáticas relacionadas con:

- Reconocimiento de amenazas comunes como phishing, ingeniería social y malware.
- Composición de contraseñas robustas (al menos 17 caracteres) y su renovación cada 3 meses.
- Administración segura de credenciales y uso de autenticación multifactor (MFA).
- Riesgos del uso de redes no seguras y descuido del puesto de trabajo.

- Recomendaciones para la clasificación, resguardo y transferencia segura de datos institucionales.

C.3. Los materiales podrán presentarse en formato digital o impreso, a través de medios institucionales como la intranet, correo electrónico o tableros informativos. La responsabilidad de consultar y aplicar dicha información recae en cada persona usuaria.

D. Formación continua

D.1. La DTIC fomentará la formación continua de todo el personal de la CONDUSEF en materia de seguridad de la información, mediante la actualización y difusión periódica de nuevos contenidos que aborden las amenazas emergentes, las mejores prácticas en protección de datos y la evolución de las tecnologías de seguridad.

D.2. La formación continua incluirá, como mínimo:

- Nuevas amenazas y técnicas de ataque que puedan surgir, como las últimas modalidades de phishing, ransomware y ataques a la seguridad en la nube.
- Actualización en los procedimientos de gestión de contraseñas y autenticación multifactor.
- Mejoras en la protección de dispositivos móviles y gestión de redes no seguras.
- Nuevas tecnologías o prácticas emergentes en seguridad informática y protección de datos

D.3. Los contenidos de formación continua estarán disponibles en formatos accesibles, como materiales en línea, seminarios web y actualizaciones de contenido a través de la CONDURED. La participación en las actividades de formación continua será recomendada para asegurar que el personal de la CONDUSEF esté al tanto de los cambios en el panorama de la seguridad de la información.

D.4. La formación continua será considerada parte integral de las responsabilidades del personal de la CONDUSEF, y su cumplimiento contribuirá al fortalecimiento de las políticas y prácticas de seguridad de la información en la CONDUSEF.

4. POLÍTICA DE GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO

A. Creación de Cuentas

A.1. La creación de cuentas de Usuario para el acceso a los recursos tecnológicos (equipos de cómputo, correo electrónico, redes y sistemas de información) será solicitada por los responsables de cada área y deberá ser aprobada por la DTIC.

A.2. Las cuentas deberán ser asignadas conforme a los roles y responsabilidades del Usuario, respetando el principio de privilegio mínimo, garantizando que el acceso se limite solo a los recursos necesarios para el desempeño de su función.

A.3. Las cuentas de Usuario serán asignadas a los Usuarios con base en una justificación laboral y autorización formal del área responsable.

A.4. Queda estrictamente prohibido el uso de cuentas genéricas o compartidas para el acceso a equipos de cómputo, correo electrónico, redes o sistemas. Cada Usuario deberá contar con una cuenta única e intransferible.

A.5. La cuenta de Usuario se protegerá mediante una contraseña, misma que deberá seguir los criterios establecidos en las presentes Políticas.

B. Control de Acceso a Sistemas y Recursos TIC´S

B.1. Acceso a Equipo de Cómputo

B.1.1. El acceso a los equipos de cómputo institucionales se realizará exclusivamente mediante cuentas personales asignadas individualmente. Cualquier excepción deberá ser formalmente documentada y autorizada por la DTIC.

B.1.2. En caso de contar con proveedores que administren equipos de cómputo institucionales, los accesos deberán estar previamente autorizados, documentados y el personal de la DTIC deberá contar con privilegios de acceso equivalentes para fines de supervisión y continuidad operativa.

B.2. Acceso a Redes

B.2.1. El acceso a la red institucional, incluidos servicios de conexión remota como VPN, será autorizado por la DTIC exclusivamente a Usuarios que lo requieran para el desempeño de sus funciones. Dicha autorización deberá estar debidamente justificada, documentada, registrada y supervisada por la DTIC.

B.2.2. El acceso remoto a los recursos institucionales estará restringido y sólo será permitido a Usuarios expresamente autorizados, en atención a criterios de confidencialidad, criticidad operativa y nivel de exposición al riesgo.

B.2.3. La administración de accesos lógicos a los activos de información se realizará mediante el uso de credenciales personales únicas, estableciendo controles de acceso acordes al perfil o rol institucional del Usuario y bajo el principio de mínimo privilegio.

B.2.4. El acceso inalámbrico estará habilitado únicamente en zonas autorizadas y se protegerá mediante protocolos de cifrados avanzados (WPA2 o superior).

B.2.5. Los dispositivos que se conecten a la red institucional deberán cumplir con los requisitos técnicos establecidos, incluyendo sistemas actualizados, herramientas de protección activa y configuraciones de seguridad validadas por la DTIC.

B.2.6. Los dispositivos móviles personales o propiedad de terceros, no podrán conectarse directamente a las redes institucionales. Cualquier conexión deberá realizarse únicamente a través de redes diferenciadas y restringidas, como la red de invitados, con acceso limitado a Internet y sin visibilidad o interacción con servicios o activos internos de la CONDUSEF.

B.2.7. Toda solicitud para la conexión de dispositivos móviles personales o propiedad de terceros a las redes institucionales deberá presentarse por escrito a la DTIC, especificando el propósito de la conexión, el periodo de tiempo requerido, el dispositivo a utilizar y el área solicitante.

B.3. Acceso al correo electrónico institucional

B.3.1. El acceso al correo electrónico institucional será autorizado únicamente a través de cuentas personales, asignadas por la DTIC con base en la relación laboral del Usuario.

B.3.2. El acceso a las cuentas deberá realizarse mediante mecanismos de autenticación seguros, incluyendo usuario y contraseña, y cuando sea aplicable autenticación multifactor.

B.3.3. La apertura de cuentas funcionales o compartidas, por ejemplo, para servicios como mesa de ayuda, atención a eventos institucionales o canales específicos de contacto deberá estar debidamente justificada y contar con la autorización formal de la DTIC. Estas cuentas deberán estar sujetas a los mismos controles de acceso y seguridad que las cuentas individuales.

B.3.4. La CONDUSEF se reserva el derecho de acceder a los correos electrónicos institucionales en casos que comprometan la seguridad de la información, en cumplimiento de auditorías o investigaciones internas autorizadas.

B.4. Acceso a aplicaciones y sistemas de información

B.4.1. El acceso a sistemas institucionales será concedido de acuerdo con el perfil del usuario y los permisos asociados a sus funciones.

B.4.2. Los privilegios serán revisados y actualizados de manera periódica o cuando cambien las funciones del Usuario.

B.4.3. Toda solicitud de acceso a sistemas deberá contar con una justificación funcional validada por el responsable del sistema o del área solicitante.

B.4.4. Las sesiones inactivas en los sistemas deberán cerrarse automáticamente tras un periodo definido por la DTIC, con base en análisis de riesgo.

B.5. La herramienta tecnológica encargada de la asignación de cuentas de Usuario y contraseñas, deberá bloquear el acceso a toda cuenta de Usuario después de 3 intentos consecutivos fallidos de acceso. Esto para cumplir con la política de bloqueo de cuentas de Usuario para cada activo, y el administrador no deberá tardar más de 1 hora en conceder acceso nuevamente al Usuario después de la explicación o justificación de olvido de contraseña o cualquier otro motivo sustentado en la no invasión de los sistemas informáticos con intenciones personales y/o de afectación a la CONDUSEF.

B.6. Todas las contraseñas para acceso con carácter administrativo deberán ser modificadas al menos cada 90 días de acuerdo a la política de seguridad establecida para evitar "ataques de fuerza bruta", "crackeadores" o cualquier otro de los métodos actuales para el intento de acceso por obtención de passwords.

B.7. El Administrador del Sistema deberá llevar a cabo un control de las cuentas de Usuario existentes y otorgadas para acceso a los Sistemas de Información, aplicaciones, redes, servidores y computadoras en cualquier sistema donde se registre y se pueda consultar el alta y baja de las mismas.

B.8. El administrador otorgará al Usuario, de acuerdo a solicitud previa del jefe inmediato por escrito o vía correo electrónico, sólo los niveles de permisos mínimos necesarios para el cumplimiento de sus actividades cotidianas

C. Suspensión y Eliminación de Cuentas

C.1. Las credenciales serán suspendidas automáticamente tras detectar inactividad mayor a 90 días, salvo justificación documentada por el área responsable. También podrán suspenderse por incidentes de seguridad, investigaciones internas o solicitud expresa de las áreas administrativas o jurídicas.

C.2. Al término de la relación laboral, contractual o de colaboración, las credenciales deberán ser eliminadas de manera inmediata en todos los sistemas donde hayan sido habilitadas. Este proceso incluirá su revocación en sistemas operativos, aplicaciones, bases de datos y servicios de red.

C.3. Se deberá llevar un registro de control en una bitácora, de todo el proceso descrito anteriormente, incluyendo motivo y fecha del alta, baja o cambio y en su caso justifique entre otros cambios.

D. Administración de Cuentas

D.1. Toda cuenta de acceso será asignada de forma individual y deberá estar vinculada a una identidad específica y verificable, evitando el uso de cuentas genéricas no justificadas.

D.2. Las credenciales de acceso son de uso personal e intransferible; su resguardo y uso adecuado serán responsabilidad exclusiva del titular.

D.3. El otorgamiento de privilegios de acceso se limitará estrictamente a lo necesario para el cumplimiento de las funciones asignadas, minimizando riesgos de exposición indebida.

D.4. Las solicitudes de alta, modificación o baja de cuentas deberán ser formalizadas mediante los canales establecidos, contar con validación del área solicitante y autorización de la DTIC.

E. Criterios para la Gestión de Contraseñas

E.1. Requisitos de seguridad

E.1.1. Las contraseñas deberán cumplir con los siguientes requisitos:

- Longitud mínima de 17 caracteres.
- Incluir al menos un carácter de los siguientes grupos:
- Letras mayúsculas
- Letras minúsculas
- Números
- Caracteres especiales (_, -, /, *, $, ¡, ¿, =, +, etc.)
- No basarse en información personal ni palabras comunes.
- No coincidir con las últimas dos contraseñas utilizadas.

E.2. Uso y protección de contraseñas

E.2.1. Los servidores deberán tratan sus contraseñas con carácter confidencial. No podrán ser escritas en papel, almacenadas en archivos ni compartidas con terceros.

E.2.2. Las contraseñas deben cambiarse cada 90 días o inmediatamente si se sospecha que ha sido comprometida.

E.2.3. Se forzará el cambio de contraseña al detectar uso repetido de contraseñas anteriores o configuración débil.

E.2.4. Se prohíbe el uso de la opción "recordar contraseña" en navegadores o aplicaciones sin aprobación del grupo de seguridad.

E.2.5. Si una contraseña es detectada como insegura, debe cambiarse de inmediato.

F. Cuentas Nuevas

F.1. Todo el personal de nuevo ingreso deberá acceder a los recursos de cómputo con una cuenta de Usuario, asignada por la DTIC a través de su área de telecomunicaciones, con el respaldo de la solicitud por escrito del jefe inmediato del Usuario, el cual será el responsable de la información.

F.2. Se entregará al Usuario una carta responsiva con sus derechos y responsabilidades de acceso, la cual deberá firmar y el Usuario aceptando los términos y condiciones de uso.

F.3. La DTIC, a través del área correspondiente de la asignación de cuentas de Usuario y contraseñas, deberá asegurar que un solo responsable, el cual tiene el rol de administrador, tenga la autoridad para la creación de accesos para cualquiera de los servicios y/o sistemas que operan dentro de la CONDUSEF y se asegurará de contar con una persona alterna que conozca el proceso para garantizar la continuidad.

5. POLÍTICA DE ADMINISTRACIÓN DE OPERACIONES Y SEGURIDAD INFORMÁTICA

A. Criterios generales

A.1. La DTIC deberá registrar, monitorear y analizar los eventos de seguridad generados en los equipos de cómputo, servidores, dispositivos de red, aplicaciones y cualquier activo de información institucional.

A.2. Los servicios de infraestructura y plataformas críticas deberán contar con planes de continuidad operativa y recuperación ante desastres (DRP/BCP).

B. Uso de Aplicaciones Institucionales

B.1. El acceso a aplicaciones institucionales que manejen información sensible deberá ser aprobado por la DTIC, quien se encargará de garantizar que los controles de seguridad estén implementados adecuadamente.

B.2. Las aplicaciones institucionales se utilizarán exclusivamente para fines laborales y relacionados con las funciones sustantivas de la CONDUSEF, queda prohibido el uso para fines personales o casos fuera de lo establecido por la CONDUSEF.

B.3. Está prohibida la instalación de complementos, extensiones o configuraciones no autorizadas que puedan alterar el funcionamiento o la seguridad de las aplicaciones.

C. Uso de Correo Electrónico

C.1. El correo electrónico institucional deberá utilizarse exclusivamente para fines relacionados con las funciones y responsabilidades laborales asignadas. Queda prohibido su uso para actividades personales, comerciales o ajenas a la operación institucional.

C.2. Se deberán aplicar configuraciones técnicas que restrinjan la entrada y salida de correos hacia o desde dominios públicos o privados no autorizados, con el fin de reducir la exposición a amenazas externas.

C.3. Queda prohibido el reenvío automático de correos electrónicos institucionales a cuentas externas no autorizadas, así como el uso compartido de credenciales o buzones sin control de acceso formalmente establecido.

C.4. La apertura de correos electrónicos, archivos adjuntos o enlaces sospechosos debe evitarse. En caso de detección de contenido malicioso, el incidente deberá ser reportado de inmediato a la mesa de ayuda de la DTIC.

C.5. Para prevenir amenazas como spam, malware o robo de datos, la DTIC implementará medidas de filtrado, detección y mitigación de correos no deseados o maliciosos, las cuales serán de observancia obligatoria para todos los Usuarios.

C.6. Las cuentas de correo temporal u operativas deberán contar con un responsable asignado y tener definidos su propósito, periodo de vigencia y controles de seguridad.

C.7. Los Usuarios deberán de abstenerse de usar cuentas de correo electrónico asignadas a otras personas, así como de recibir mensajes en cuentas de otros.

C.8. Los Usuarios deberán tratar los correos electrónicos institucionales y sus archivos adjuntos como una comunicación privada y directa entre emisor y receptor, observando para esos efectos las obligaciones en el manejo de información reservada, confidencial.

C.9. Queda estrictamente prohibido el uso y/o vinculación del correo electrónico institucional en clientes de correo como Gmail, Yahoo, Hotmail, etc., toda vez que el acceso a estos servicios quedará bloqueado a partir de la entrada en vigor de las presentes Políticas de Seguridad de la Información. En los casos específicos con necesidad de los anteriores servicios, en primera instancia será solicitado dicho acceso al Director del Usuario para su revisión y si ésta es autorizada, el titular de la Unidad Administrativa correspondiente solicitará por escrito a la DTIC dicha solicitud

D. Uso de Internet

D.1. El acceso a Internet deberá utilizarse exclusivamente para el cumplimiento de funciones institucionales, conforme a las atribuciones del personal y los fines de la CONDUSEF.

D.2. Queda prohibido el acceso a sitios web con contenidos inapropiados, ilegales, no relacionados con las funciones institucionales, o que representen un riesgo para la seguridad de la información. Los Usuarios de Internet de la CONDUSEF deberán avisar inmediatamente a la DTIC, por la mesa de ayuda, cualquier incidente que pudiere afectar la Seguridad de la Información de la CONDUSEF.

D.3. La navegación en Internet deberá realizarse a través de la infraestructura institucional autorizada, la cual contará con filtros, registros y mecanismos de control implementados por la DTIC.

D.4. No está permitido el uso de servicios en la nube no autorizados, plataformas de almacenamiento personal o aplicaciones web que impliquen la transferencia de información institucional fuera del entorno controlado por la CONDUSEF.

D.5. El personal de la CONDUSEF deberá abstenerse de descargar, instalar o ejecutar archivos provenientes de fuentes no verificadas o no oficiales, salvo autorización de la DTIC.

D.6. Se prohíbe la utilización de redes privadas virtuales (VPN) no institucionales o herramientas que oculten la identidad del Usuario o modifiquen las políticas de conexión de la red institucional.

D.7. Toda actividad de navegación en Internet está sujeta a monitoreo, registro y análisis por parte de la DTIC, con el fin de prevenir incidentes de seguridad, cumplir con la normativa vigente y garantizar el uso adecuado de los recursos.

D.8. El uso de redes sociales y plataformas digitales está permitido únicamente en los casos en que sea requerido por funciones específicas autorizadas, y deberá realizarse con apego a los principios de confidencialidad, integridad y disponibilidad de la información institucional.

D.9. Queda estrictamente prohibido intentar evitar, desactivar o vulnerar los mecanismos de control establecidos para el acceso, filtrado y seguridad en la navegación por Internet. Todo acceso deberá realizarse conforme a los lineamientos de seguridad establecidos por la DTIC.

D.10. La DTIC establecerá los mecanismos de restricción, segmentación y control del tráfico de red para garantizar la protección de los activos de información durante el uso de Internet.

E. Seguridad del Equipo de Cómputo

E.1. Los equipos de cómputo asignados por la CONDUSEF deberán ser utilizados exclusivamente para fines institucionales y conforme a las funciones y responsabilidades del personal al que se asignen.

E.2. La DTIC será responsable de generar imágenes de instalación base con software autorizado, preferentemente software libre, conforme al perfil y rol funcional del usuario, siguiendo el principio de menor privilegio.

E.3. Si el Usuario por la naturaleza de sus actividades requiere viajar constantemente o trabaja en lugares públicos, deberá considerar la posibilidad de tener accesos a la red privada virtual (VPN) de la CONDUSEF. Para este caso deberá de solicitar una cuenta de Usuario para el acceso a la VPN a la DTIC, quién será la responsable de analizar la procedencia conforme la justificación que realice el titular del área en la que el Usuario realice sus actividades.

E.4. La DTIC implementará herramientas de monitoreo para detectar software no autorizado, actividades inusuales y posibles amenazas que comprometan la seguridad de los equipos institucionales.

E.5. Se aplicarán controles para impedir la desinstalación o desactivación de software y servicios de seguridad instalados en los equipos de cómputo.

E.6. Todos los equipos deberán contar con soluciones antimalware activas y actualizadas, así como con firewalls configurados para bloquear tráfico no autorizado. Su desactivación solo podrá realizarse por personal autorizado y con justificación documentada.

E.7. Se deberán restringir los privilegios de ejecución de herramientas de línea de comandos como PowerShell, Terminal o Shell, a Usuarios autorizados mediante políticas de grupo.

F. Mecanismos contra Código Malicioso

F.1. Para prevenir infecciones por virus informáticos, los Usuarios de la CONDUSEF deberán abstenerse de hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la DTIC.

F.2. El Usuario deberá verificar que todos los archivos electrónicos que le sean proporcionados por un Tercero o personal de la DTIC, considerando al menos programas de software, bases de datos, documentos, hojas de cálculo y cualquier otro archivo que tengan que ser descomprimidos, estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

F.3. Los Usuarios deberán abstenerse de escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir códigos de computadora diseñados para autorreplicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software, así como de probarlos en cualquiera de los ambientes o plataformas de la CONDUSEF. El incumplimiento de este criterio será considerado una falta grave a la Seguridad de la Información de esta Comisión Nacional.

F.4. Ningún Usuario, o Tercero deberá bajar o descargar software, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la autorización expresa de la DTIC.

G. Dispositivos Móviles

G.1. El uso de dispositivos de cómputo o móviles personales de los Usuarios con acceso a la red y los servicios y aplicaciones de la CONDUSEF es exclusivamente para las actividades relacionadas con las necesidades del puesto y/o actividad que desempeña.

G.2. La asignación del acceso a la red y los servicios y aplicaciones de la CONDUSEF, a través de cualquier dispositivo de cómputo o móvil personal, deberá solicitarse a la DTIC, señalando los motivos por los que se requiere el acceso.

G.3. Los Usuarios de dispositivos de cómputo o móviles personales, que hacen uso de la red de los servicios y de las aplicaciones de la CONDUSEF, deberán avisar de forma inmediata a la DTIC de cualquier incidente que pudiere afectar la Seguridad de la Información de esta Comisión Nacional.

G.4. Se considerará que los Usuarios de dispositivos de cómputo o móviles personales de la CONDUSEF, cuando se les proporcione acceso a la red, así como a los servicios y aplicaciones de esta Comisión Nacional, tendrán conocimiento y aceptarán que:

G.4.1. Serán sujetos de monitoreo de las actividades que realice en su dispositivo.

G.4.2. Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.

G.5. Se prohíbe el almacenamiento de archivos personales, en las unidades de red asignadas al Usuario, o en el equipo de cómputo a su cargo, debido a que estos recursos son de uso exclusivo para el cumplimiento de sus funciones/actividades en la CONDUSEF, y así mismo porque puede tratarse de archivos que contengan amenazas informáticas como códigos maliciosos.

G.6. La DTIC deberá de llevar un registro y control de todos los dispositivos móviles que posee la CONDUSEF.

G.7. Definir un procedimiento formal de salida de dispositivos de las instalaciones, únicamente se permitirá a Usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del jefe inmediato.

G.8. Los dispositivos móviles que son autorizados para salir de las instalaciones por la Dirección de Recursos Materiales y Servicios Generales, deben ser protegidos mediante el uso e implementación de los controles apropiados para ello, como son: cifrado de información, políticas de restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN.

G.9. Todos los dispositivos propiedad de la CONDUSEF, como celulares que almacenen información de la CONDUSEF, deben contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave.

G.10. Todos los dispositivos móviles propiedad de la CONDUSEF pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

G.11. Queda estrictamente prohibido el uso de cámaras o grabadoras móviles para grabar información confidencial relacionada con la CONDUSEF.

H. Servicios de Telefonía

H.1. Todas las líneas telefónicas son de uso oficial para el cumplimiento de las funciones/actividades encomendadas al personal de la CONDUSEF; por lo que no podrán ser utilizadas como líneas privadas o para fines personales.

I. Equipo Desatendido

I.1. Los Usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla cuando no se encuentren en su lugar de trabajo.

I.2. Los Usuarios no podrán alterar la configuración del equipo asignado aprovechando su conocimiento sobre Aplicativos Informáticos para establecer una condición de uso favorable o en beneficio personal.

I.3. Los Usuarios no deberán mover o reubicar los equipos de cómputo, periféricos, de telefonía o telecomunicaciones, instalar o desinstalar dispositivos sin la autorización de la DTIC.

I.4. Queda prohibido que el Usuario abra o desarme los equipos de cómputo y de telefonía.

6. POLÍTICA PARA EL DESARROLLO SEGURO DE SOFTWARE

A. Seguridad en el Ciclo de Desarrollo de Software

A.1. Integración de requisitos de seguridad desde la etapa de análisis: Todos los proyectos de desarrollo deberán incorporar requisitos de seguridad desde su planeación, incluyendo criticidad de la información que manejará, impacto en la continuidad operativa ante una falla o vulnerabilidad, controles para la protección de datos personales, acceso restringido, cifrado y trazabilidad de eventos relevantes.

A.2. Los aplicativos informáticos deberán implementar controles para validar la información ingresada por los usuarios, así como mecanismos seguros de gestión de errores para evitar fugas de información sensible.

A.3. Cualquier dato clasificado como confidencial, en tránsito o en almacenamiento, deberá ser protegido mediante algoritmos de cifrado adecuados.

A.4. Toda solución desarrollada debe incorporar mecanismos de autenticación y autorización seguros, tales como:

- A.4.1. Controles de autenticación robustos, preferentemente con autenticación multifactor.
- A.4.2. Gestión de permisos conforme al principio de mínimo privilegio.
- A.4.3. Registro de accesos y permisos.

A.5. El código fuente debe estar resguardado en entornos controlados, con acceso limitado a personal autorizado, registrando todo acceso y modificación.

A.6. No se debe incluir información confidencial (como contraseñas, tokens, claves privadas o configuraciones críticas) directamente en el código fuente.

A.7. Se prohíbe la inclusión de mecanismos de acceso no documentados o controlados que permitan eludir controles de autenticación o autorización.

A.8. Se deberá utilizar, cuando sea posible, herramientas de análisis que permitan identificar vulnerabilidades de seguridad en el código antes de su implementación.

B. Gestión Segura de Componentes Externos

B.1. Se debe verificar que cualquier componente de software externo (como librerías, frameworks o plugins) provenga de fuentes confiables, esté actualizado y libre de vulnerabilidades conocidas.

B.2. En caso de integrar APIs, interfaces o fuentes de datos externas, se deberá garantizar que cuenten con medidas de seguridad, documentación completa y estén contempladas como parte del análisis de riesgos del proyecto.

B.3. Se deberán aplicar buenas prácticas de gestión de dependencias, incluyendo el monitoreo continuo de avisos de seguridad y actualizaciones críticas.

C. Gestión Segura de Ambientes de Desarrollo y Pruebas

C.1. Los entornos de desarrollo, pruebas y producción deben estar segregados para evitar accesos no autorizados y garantizar la integridad de la información.

C.2. Está prohibido utilizar datos reales de usuarios en ambientes de prueba. Se deben emplear datos simulados o anonimizados para preservar la privacidad de la información.

C.3. Toda liberación de código o implementación en ambientes de pruebas o producción deberá ser realizada exclusivamente por personal autorizado, ejecutarse desde ubicaciones y equipos seguros, estar debidamente documentada y ser validada por el área responsable del aseguramiento de la calidad o de la seguridad de la información.

7. POLÍTICA DE CLASIFICACIÓN Y GESTIÓN DE LA INFORMACIÓN

A. Clasificación y Etiquetado de la Información

A.1. Toda la información generada, procesada, almacenada o transmitida por la CONDUSEF deberá clasificarse con base en su sensibilidad, criticidad y riesgo asociado a su divulgación no autorizada. Esta clasificación deberá realizarse desde su origen y revisarse periódicamente para garantizar su vigencia y pertinencia.

A.2. La información institucional será clasificada, como mínimo, en las siguientes categorías:

A.2.1. Pública: Información que puede ser divulgada sin restricciones.
A.2.2. De uso interno: Información de circulación limitada dentro de la institución.
A.2.3. Confidencial: Información cuyo acceso debe restringirse por implicaciones legales, regulatorias o estratégicas.

A.3. La información deberá ser clasificada:

A.3.1. Al momento de su creación, recepción o modificación significativa.
A.3.2. Cuando se reciba una solicitud de acceso y el documento no cuente con clasificación previa.
A.3.3. Al revisar los archivos o repositorios de forma periódica como parte de auditorías o revisiones internas.

A.4. El etiquetado de la información deberá realizarse de forma clara, utilizando marcas visuales o metadatos digitales, y contemplará tanto documentos en formato físico como electrónico.

A.5. Los Usuarios deberán conocer de manera clara y precisa que existe una clasificación y etiquetado de la información asignada como pública, reservada y confidencial, a la cual deben asignarle una protección apropiada.

A.6. La CONDUSEF, deberá adoptar las medidas necesarias para asegurar la custodia y conservación de los expedientes clasificados.

A.7. La DTIC, deberá tener conocimiento y llevar un registro de los servidores públicos que, por la naturaleza de sus atribuciones, tengan acceso a los expedientes y documentos clasificados como reservados o confidenciales. Asimismo, deberá asegurarse que dichos servidores públicos tengan conocimiento de la responsabilidad en el manejo de información clasificada.

B. Protección de Información Confidencial

B.1. Toda la información clasificada como confidencial deberá protegerse mediante controles físicos, administrativos y técnicos adecuados a su nivel de sensibilidad, incluyendo medidas como:

B.1.1. Control de acceso con base en perfiles de usuario.

B.1.2. Cifrado de archivos y medios de almacenamiento.
B.1.3. Monitoreo de accesos y trazabilidad de modificaciones.
B.1.4. Uso de herramientas seguras para su transmisión (correo cifrado, VPN, etc.).

B.2. Las personas servidoras públicas deberán estar informadas de las responsabilidades inherentes al manejo de información clasificada. Se deberá garantizar que:

B.2.1. El personal que acceda a información clasificada cuente con la autorización correspondiente.
B.2.2. Se conserve evidencia documental de dicha autorización (cartas responsivas o acuerdos de confidencialidad).
B.2.3. Se proporcionen lineamientos claros sobre la manipulación, reproducción, transferencia y eliminación de información clasificada.

B.3. Está estrictamente prohibida la divulgación no autorizada de cualquier activo de información, sin importar el medio de acceso (sistemas institucionales, correo electrónico, copias impresas, entre otros).

B.4. Las áreas deberán contar con procedimientos documentados para la protección y conservación de expedientes clasificados, incluyendo mecanismos para su respaldo, recuperación ante desastres y destrucción segura al final de su ciclo de vida.

8. POLÍTICA DE GESTIÓN DE ACTIVOS

A. Identificación y Registro de Activos de Información

A.1. Todos los activos de información que son utilizados, generados, procesados, almacenados o transmitidos por la CONDUSEF deben ser identificados, registrados y gestionados de forma adecuada para garantizar su protección, disponibilidad y trazabilidad.

A.2. El inventario de activos deberá contener información detallada y debe incluir tanto activos físicos como digitales:

A.2.1. Equipos de cómputo, periféricos, impresoras y dispositivos móviles.

A.2.2. Medios de almacenamiento (discos duros, memorias USB, servidores).
A.2.3. Dispositivos de comunicación y telecomunicaciones.
A.2.4. Software, licencias, configuraciones, código fuente y desarrollos internos.
A.2.5. Documentación técnica y medios impresos.

A.3. La DTIC será responsable de mantener actualizado el inventario de activos, asegurando su disponibilidad para fines operativos, de auditoría, legales o financieros.

A.4. Los custodios de la información serán responsables de aplicar los procedimientos de control específicos, administrar el control de acceso a la información y suministrar capacidades de recuperación, en concordancia con las instrucciones y definiciones de los propietarios de la información.

A.5. Todos los Activos de Información serán exclusivamente para el cumplimiento de las funciones de la CONDUSEF y deberán estar protegidos de acuerdo con su importancia y valor.

A.6. Todos los Activos de Información deberán tener un propietario (dueño). Dicho propietario será responsable de garantizar la Integridad, Confidencialidad y Disponibilidad de la Información.

A.7. Los dueños de los Activos de Información deberán aceptar por escrito la propiedad de sus activos describiendo conjuntamente su responsabilidad sobre éstos. Los propietarios de activos podrán delegar algunas responsabilidades, en el ámbito de su competencia, sobre sus activos a persona o entidad a quien se le reconocerá como "Custodio".

B. Uso Aceptable de Activos de Información

B.1. Los activos de información deben utilizarse exclusivamente para el cumplimiento de las funciones institucionales de la CONDUSEF. Cualquier otro uso deberá contar con autorización expresa de la DTIC.

B.2. El personal deberá utilizar los activos conforme a los lineamientos y restricciones definidos por la CONDUSEF, evitando acciones que comprometan su integridad, confidencialidad o disponibilidad.

B.3. Solo personal autorizado podrá realizar reparaciones, mantenimiento o intervención sobre equipos informáticos o de telecomunicaciones. El personal usuario deberá verificar la identidad y autorización del personal técnico antes de permitir el acceso a los equipos.

B.4. Se deberá acordar y documentar para cada uno de los activos el tipo de clasificación que le corresponde. Es necesario, identificar los niveles de protección que le corresponden acorde con la importancia de los activos a través del análisis de riesgos.

B.5. Los inventarios de activos deberán estar actualizados y documentados para propósitos de la CONDUSEF, legales o financieros.

B.6. Los Activos de Información bajo la responsabilidad de CONDUSEF, deberán ser administrados y actualizados.

C. Gestión de Responsabilidades Sobre Activos

C.1. El propietario del activo podrá delegar algunas funciones relacionadas con la administración o resguardo del mismo a un custodio, sin que ello implique deslinde de su responsabilidad general.

C.1.1. La aceptación de responsabilidades como propietario de un activo deberá ser documentada formalmente. Esta aceptación implicará el compromiso de garantizar su integridad, confidencialidad y disponibilidad, así como el cumplimiento de los controles definidos por la normativa institucional.

C.1.2. Los custodios designados por los propietarios de los activos deberán aplicar los controles de seguridad que les correspondan, incluyendo la administración del acceso autorizado, el monitoreo del uso adecuado y la implementación de mecanismos de respaldo y recuperación de la información.

C.2. En caso de uso inapropiado de activos, la DTIC podrá restringir temporal o permanentemente el acceso a los recursos involucrados, conforme a la normativa interna y procedimientos aplicables.

D. Devolución y baja de activos

D.1. Al término de la relación laboral, contractual o de colaboración, las personas servidoras públicas, prestadores de servicios o terceros deberán devolver todos los activos que hayan tenido bajo su responsabilidad.

D.2. La DTIC, en coordinación con las áreas correspondientes, deberá verificar que se haya realizado la devolución total de los activos asignados y documentar dicho proceso.

D.3. La DTIC deberá mantener registros de los activos devueltos y dados de baja, con fines de control interno, transparencia y auditoría.

E. Responsabilidad sobre los Activos

E.1. La DTIC deberá establecer los criterios de uso de los recursos informáticos para protegerlos y promover su uso óptimo.

E.2. Todos los activos deberán ser inventariados y se deberá asignar la responsabilidad de su uso al servidor público, mediante un documento de resguardo.

E.3. La implementación de controles específicos podrá ser delegada en caso de ser necesario y/o apropiado, pero el propietario seguirá siendo responsable por la protección de los activos.

F. Devolución de los Activos

F.1. Para la devolución de Activos de Información, deberá realizarse la entrega de estos por parte de los servidores públicos, prestadores de servicios y Terceros que tengan bajo su responsabilidad, a fin de garantizar la Confidencialidad, Integridad y Disponibilidad de los Activos al término del empleo contrato o acuerdo.

F.2. La DTIC, deberá establecer responsabilidades para asegurarse de la correcta gestión de la salida de los servidores públicos, prestadores de servicios o terceros; así mismo, deberá cerciorarse de la completa devolución de todo el equipo.

9. POLÍTICA DE MANEJO Y ELIMINACIÓN SEGURA DE MEDIOS

A. Borrado Seguro

A.1. El borrado seguro es obligatorio para todo dispositivo que contenga o haya contenido información institucional clasificada como confidencial, ya sea, financiera, patrimonial o datos personales.

A.2. El procedimiento de borrado seguro deberá garantizar que la información no pueda ser recuperada por ningún medio técnico disponible.

A.3. El personal responsable del borrado deberá contar con autorización expresa de la DTIC, para realizar el procedimiento correspondiente.

A.4. En el caso de infraestructura gestionada por proveedores, estos deberán ejecutar el procedimiento de borrado seguro al momento de realizar sustituciones, al término del contrato.

A.5. Las memorias USB o cualquier otro dispositivo de almacenamiento portátil, no deberán ser usadas como medios formales para conservar respaldos con cualquier tipo de información.

A.6. Las memorias USB o cualquier otro dispositivo de almacenamiento portátil, que se encuentre dentro de las instalaciones de la CONDUSEF, podrán ser revisadas en cualquier momento por el RSI de la Comisión Nacional.

A.7. Las memorias USB o cualquier otro dispositivo de almacenamiento portátil que contenga información de datos personales y datos personales sensibles, financieros, patrimoniales o clasificada como confidencial o reservada de la CONDUSEF, se deberá de encontrar cifrada con los mecanismos autorizados por la DTIC para evitar el acceso a dicha información en caso de robo o extravío del dispositivo.

A.8. La transmisión de la información por medios físicos requiere de los siguientes controles:

A.8.1. La información deberá ser liberada exclusivamente a las personas autorizadas definidas por el propietario de la información.

A.8.2. La transmisión de la información, deberá darse con controles que no permitan la intercepción de parte de Usuarios no autorizados que pongan en riesgo la Confidencialidad de la Información. Para ello, uno de los siguientes controles puede ser implementado:

- Si la información es trasladada por una persona o si es enviada por mensajería, la información deberá ser etiquetada y almacenada en un recipiente de tal forma que no se observe en el recipiente el nivel de clasificación de la información, y ningún dato relacionado con la información contenida.

- Si la Información es trasladada por una persona, o si es enviada por mensajería, y si además puede ser almacenada en un medio electrónico (USB o CD) la información deberá ser cifrada con los mecanismos autorizados por la DTIC, para prevenir el acceso y manipulación de la información por personas no autorizadas.

- El propietario de la información, deberá de dar seguimiento para verificar que la información se recibió sin ningún incidente.

B. Gestión de Dispositivos de Almacenamiento de Datos

B.1. El uso de dispositivos portátiles de almacenamiento (memorias USB, discos externos, CD/DVD, tarjetas SD u otros) debe restringirse al mínimo indispensable.

B.2. Queda prohibido almacenar, transportar o extraer de las instalaciones información institucional clasificada como confidencial sin que el medio esté debidamente cifrado.

B.3. No se permite la conexión de dispositivos de origen desconocido o encontrados abandonados, a ningún equipo institucional.

B.4. Los dispositivos portátiles no podrán utilizarse como medio de respaldo formal de información. Los respaldos deben realizarse únicamente mediante los mecanismos centralizados definidos por la DTIC.

B.5. Los dispositivos portátiles de almacenamiento que contengan información institucional podrán ser revisados en cualquier momento por el RSI o la DTIC.

C. Eliminación de Datos en Dispositivos de Almacenamiento Externo

C.1. La disposición o destrucción de información deberá definirse de manera que prevenga el acceso, y manipulación de la información por personas no autorizadas.

C.2. Queda prohibido reutilizar o reciclar dispositivos de almacenamiento que hayan contenido información con nivel de clasificación alto o confidencial, sin aplicar previamente un borrado seguro.

C.3. La destrucción de información contenida en medios físicos (papel), electrónicos o magnéticos deberá realizarse de forma que garantice no sean legibles, ni recuperables por terceros. Los métodos utilizados deberán cumplir con los procedimientos y estándares autorizados por la DTIC, a fin de prevenir cualquier riesgo de divulgación de datos residuales.

C.4. Las características de destrucción de la información, deberán ser las autorizadas por la DTIC para asegurar que no existen riesgos de divulgación para datos residuales en dispositivos físicos, electrónicos, o magnéticos.

D. Soportes Físicos en Tránsito

D.1. El traslado de información en medios físicos deberá ser realizado por personal expresamente autorizado por el propietario de la información o la DTIC y bajo medidas que eviten el acceso, pérdida, exposición o manipulación por parte de terceros.

D.2. Cuando la información se transmita en medios electrónicos portátiles (como USB o CD), deberá estar cifrada con herramientas autorizadas por la DTIC.

D.3. El responsable de la información deberá dar seguimiento al proceso hasta confirmar su recepción segura por parte del destinatario.

10. POLÍTICA DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

A. Sistemas, Activos y Herramienta a Respaldar

A.1. La DTIC, en coordinación con las áreas usuarias, deberá identificar los sistemas, aplicativos y activos de información clasificados como críticos para el funcionamiento institucional, mismos a los que se les dará prioridad en la generación y protección de respaldos.

A.2. La criticidad de los activos deberá ser revisada periódicamente, especialmente en procesos de actualización tecnológica o reorganización institucional.

B. Generación y Gestión de Respaldos

B.1. La DTIC deberá establecer políticas de respaldo automatizadas para los sistemas críticos, incluyendo respaldos completos e incrementales, según la periodicidad y volumen de datos.

B.2. Los respaldos deberán incluir metadatos que permitan su trazabilidad, tales como: fecha de generación, tipo de respaldo, contenido y sistema origen.

B.3. Toda información respaldada deberá estar debidamente cifrada, con el fin de proteger la confidencialidad e integridad de los datos.

B.4. La información respaldada deberá almacenarse de forma redundante.

B.5. Los respaldos deberán conservarse de acuerdo con la clasificación de la información y los plazos establecidos en la normativa aplicable en materia de archivos, protección de datos personales y seguridad de la información.

B.6. Se realizarán pruebas periódicas de restauración para verificar la integridad de los respaldos y asegurar la operatividad de los procedimientos de recuperación.

B.6.1. Las pruebas de restauración deberán formar parte del proceso de mejora continua del BCP y del DRP institucional.

B.6.2. Los resultados de las pruebas deberán documentarse, y en caso de inconsistencias, deberán tomarse medidas correctivas de manera inmediata.

C. Estándares Aprobados para el Borrado Seguro

C.1. La herramienta de destrucción digital de datos, deberá cumplir con al menos tres de los estándares que se describen a continuación:

- DOD 5220.22-M
- NAVSO P-5239-26
- NCSC-TG-025
- NSA 130-1
- Bruce Schneier´s algorithm
- Peter Gutmann´s algorithm
- Opnavinst5239.1ª
- HMG Infosec Standard 5, Lower Standard
- HMG Infosec Standard 5, Higher Standard
- NIST 800-88 / ATA Secure Erase (+ assurance)
- CESG CPA – Nivel Superior
- BSI-GS
- BSI-2011-VS
- AFSSI-5020
- RCMP TSSIT OPS-II
- CSEC ITSG-06
- ISM 6.2.92
- NZSIT 402
- VSITR
- GOST R 50739-95
- Pfitzner

D. Certificación de la Herramienta

D.1. La herramienta de destrucción digital de datos deberá tener al menos una de las siguientes certificaciones:

- NSTL
- OTAN
- COMMON CRITERIA

E. Información a Integrar en el Reporte

E.1. La herramienta utilizada por el proveedor del servicio, para el Borrado de datos, al finalizar el contrato, deberá generar por cada uno de los equipos borrados un reporte que certifique el proceso de Borrado, conteniendo al menos la siguiente información y características:

- Reporte Protegido Digitalmente.
- Firma Digital.
- Fecha del Reporte.
- Número del Reporte.
- Información de Disco.
- Información del Equipo.
- Estatus de Terminación del Proceso de Borrado.
- Duración del Borrado.
- Campos de Impresión para Firmas de quien ejecuta el Borrado y quien recibe el Reporte.

F. Excepciones

F.1. El Borrado seguro no se realizará a dispositivos finales o de Usuario, solo se ejecutará en los servidores que forman parte del servicio de renovación tecnológica de cómputo central.

11. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

A. Protección y Mantenimiento de Equipos Críticos

A.1. Todos los equipos que conforman la infraestructura tecnológica crítica de la CONDUSEF deberán ser objeto de mantenimiento preventivo y correctivo conforme a los lineamientos del fabricante y a la normativa interna.

A.2. El mantenimiento lógico y físico deberá ser programado y notificado con antelación a las áreas usuarias, minimizando el impacto en la operación institucional.

A.3. Solo personal autorizado, debidamente calificado e identificado podrá realizar actividades de mantenimiento sobre equipos de cómputo, telecomunicaciones, redes eléctricas, cableado estructurado, sistemas de enfriamiento o energía.

A.4. Los sistemas de energía eléctrica (UPS, plantas de emergencia), detección y supresión de incendios y climatización deberán recibir mantenimiento preventivo y pruebas periódicas documentadas.

A.5. Deberán mantenerse registros detallados de todos los mantenimientos realizados, fallas detectadas y acciones correctivas implementadas.

A.6. Todo equipo que sea retirado temporalmente para su reparación deberá quedar registrado, indicando el motivo, ubicación y responsable del resguardo.

A.7. La DTIC o el área responsable deberá implementar procedimientos que garanticen el mantenimiento, resguardo, adecuación y sanitización segura de estaciones de trabajo y equipos portátiles, protegiendo la disponibilidad, integridad y confidencialidad de la información.

B. Seguridad de los Equipos Fuera de las Instalaciones

B.1. El traslado, reubicación o retiro de equipos fuera de los inmuebles de la CONDUSEF deberá contar con autorización previa del área responsable y ser registrado en la bitácora correspondiente.

B.2. Para la salida física de dispositivos institucionales de las instalaciones, deberá existir un procedimiento documentado. Solo se permitirá la salida a personas servidoras públicas autorizadas.

B.3. Todo dispositivo móvil autorizado para salir de las instalaciones deberá contar con controles de seguridad adecuados, entre ellos:

B.3.1 Cifrado de la información almacenada.

B.3.2. Restricciones sobre la instalación y ejecución de aplicaciones.

B.4. El uso de dispositivos fuera de las instalaciones deberá ser previamente autorizado por la DTIC y estar sujeto a controles de seguridad acordes con el nivel de sensibilidad de la información que contienen.

B.5. Se deberán implementar mecanismos de control para asegurar el trabajo remoto o móvil, incluyendo conexión segura (VPN) a los sistemas institucionales y monitoreo de actividad conforme a los lineamientos aplicables.

B.6. Siempre que se utilice cifrado, las llaves empleadas deberán ser generadas para que no puedan ser replicables, y que sean difíciles de descifrar. El uso de llaves de cifrado de mayor número de "bits" (AES de 128 comercialmente) deberá ser el preferido.

B.7. La información reservada y confidencial que el RSI establezca, deberá ser cifrada utilizando los procedimientos definidos en la presente Política.

B.8. Las llaves de cifrado utilizadas no deberán ser compartidas con ningún Tercero, a menos que se cuente con la autorización del RSI.

B.9. Todo el proceso de la administración de llaves será auditable.

B.10. Se implementará el uso de bitácoras en el sistema de administración de llaves.

B.11. Deberá existir un procedimiento para la destrucción segura de las llaves, el cual contemplará la autorización del RSI con el fin de validar el correcto apego a la presente Política.

C. Control y Acceso Físico a los Activos de Información Esenciales

C.1. Se deberán establecer controles físicos que restrinjan el acceso a personal no autorizado, tanto internas como externas, a instalaciones donde se resguarden medios de almacenamiento, activos de información esenciales o infraestructura crítica.

C.2. Toda entrada al Centro de Datos o a áreas con acceso a información clasificada deberá registrarse en una bitácora de control físico, la cual debe incluir:

- Nombre del servidor público o visitante autorizado.
- Fecha y hora de ingreso
- Fecha y hora de salida.
- Actividad realizada.
- Firma del responsable.

C.3. Se deberán implementar medidas para prevenir daños físicos o interferencias en instalaciones y áreas críticas, incluyendo:

C.3.1. Protección eléctrica: Uso de tomas de tierra, reguladores de voltaje y sistemas de alimentación ininterrumpida (UPS).

C.3.2. Prevención de incendios: Instalación de sistemas automáticos de detección y supresión de incendios adecuados para equipos electrónicos.

C.3.3. Control de temperatura: Los equipos deberán operar en ambientes controlados.

12. POLÍTICA DE GESTIÓN DE TERCEROS

A. Evaluación y Supervisión de Proveedores de TI

A.1. Todo proveedor que ofrezca servicios relacionados con Tecnologías de la Información deberá ser evaluado previamente por la DTIC, considerando criterios de capacidad

técnica, cumplimiento normativo, prácticas de seguridad y continuidad del servicio.

A.2. La CONDUSEF deberá mantener un registro actualizado de todos los proveedores contratados para servicios de TI, incluyendo los permisos otorgados, accesos habilitados, responsables asignados y activos involucrados.

A.3. Los proveedores deberán facilitar la documentación que la CONDUSEF requiera para la realización de auditorías internas, revisiones técnicas o procesos de supervisión.

A.4. La CONDUSEF podrá realizar auditorías y evaluaciones a los proveedores en cualquier momento durante la vigencia del contrato, a fin de verificar el cumplimiento de los acuerdos establecidos y los controles de seguridad requeridos.

A.5. Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deberán ser realizados por personal especialista y debidamente autorizado e identificado.

A.6. Se deberán realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de energía (UPS y/o plantas eléctricas), sistemas de detección y extinción de incendios y del sistema de enfriamiento.

A.7. Se deberán realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la CONDUSEF.

A.8. Se deberá proveer un procedimiento, que garantice la realización del mantenimiento preventivo y correctivo de las estaciones de trabajo y equipos portátiles, así como su adecuación para la reutilización o reasignación de manera segura en el cual se conserve la Disponibilidad, Integridad y Confidencialidad de la información contenida en los mismos.

A.9. El RSI, deberá garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad, así como las redes de comunicaciones se encuentran protegidos.

A.10. Deberán quedar registradas todas las fallas supuestas o reales, así como todo el mantenimiento preventivo y correctivo realizado.

A.11. Deberá registrarse la salida de los equipos que, por su estado, haya sido necesario retirar de las instalaciones de la CONDUSEF para su mantenimiento.

A.12. Se deberá monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del centro de cómputo, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

B. Prestadores de Servicios

B.1. Todo proveedor deberá designar representantes de contacto técnico y administrativo que atiendan requerimientos, cambios o incidentes relacionados con el servicio contratado.

B.2. Los proveedores deberán identificar los activos que utilizarán para la prestación del servicio y reportarlos a la DTIC, indicando el periodo de uso requerido y justificando los accesos solicitados.

B.3. La información y los activos a los que accedan los terceros deberán estar claramente identificados y ser supervisados por personal autorizado de la CONDUSEF.

B.4. El acceso físico o lógico de terceros a infraestructura institucional deberá contar con autorización formal del personal pertinente y sujetarse a los controles de seguridad establecidos.

B.5. Los equipos de cómputo móviles (laptops) usados fuera de las instalaciones de CONDUSEF que resguarden información "restringida y/o confidencial", deberán mantener las siguientes medidas de seguridad:

B.5.1. Contar con un software autorizado para cifrar toda la información confidencial.
B.5.2. Emplear una VPN para su comunicación con los sistemas institucionales.
B.5.3. Emplear una contraseña robusta para el inicio de la sesión y arranque del sistema operativo.

B.6. Se deberá considerar el uso de seguros contra robo, pérdida de los equipos de cómputo, entre otros.

C. Tratamiento de la Seguridad en Contratos con Terceros

C.1. Todo contrato formalizado con proveedores que accedan, procesen o custodien información institucional deberá contener cláusulas específicas sobre la protección de la información, las responsabilidades en caso de incidentes y las sanciones aplicables por incumplimiento.

C.2. Los proveedores deberán firmar un Acuerdo de Confidencialidad antes de iniciar cualquier actividad, en el que se establezcan al menos las siguientes obligaciones:

- No divulgar información sensible o clasificada a la que tengan acceso.
- Compromiso de cumplimiento con la normativa interna aplicable.
- Mantener la confidencialidad de la información durante el tiempo estipulado.
- Duración de la obligación de confidencialidad, incluso posterior al término del contrato.
- Sanciones por incumplimiento.

C.3. El proveedor deberá comprometerse a utilizar canales seguros de comunicación y abstenerse de compartir información institucional a personal no autorizado o ajeno al proyecto.

C.4. En caso de terminación del contrato, el proveedor deberá devolver, eliminar o destruir toda la información institucional a la que haya tenido acceso, conforme a los procedimientos establecidos por la DTIC y la normativa vigente.

D. Gestión de Proveedores

D.1. La CONDUSEF notificará a los proveedores los lineamientos, políticas y controles de seguridad vigentes, los cuales deberán ser aceptados y cumplidos por estos en el marco de sus actividades.

D.2. Todo acceso concedido a terceros será temporal y deberá limitarse al mínimo indispensable, revocándose una vez concluido el servicio o proyecto correspondiente.

D.3. Los proveedores de servicios críticos o que manejen datos personales o información clasificada deberán contar con un Plan de Continuidad de Negocio y/o Plan de Recuperación ante Desastres (DRP), alineado a los lineamientos establecidos por la CONDUSEF.

13. POLÍTICA DE RESPALDOS

A. Sistemas, Activos y Herramientas a Respaldar

A.1. Se deberán identificar las aplicaciones críticas para dar prioridad a la generación y protección de dichos respaldos.

A.2. Los aplicativos y activos identificados como críticos, deberán ser tomados en consideración para la elaboración del Plan de Continuidad del Negocio (BCP) y del Plan de Recuperación de Desastres (DRP).

B. Generación de Respaldos

B.1. Se deberán establecer y configurar políticas de respaldo en los servidores de las aplicaciones críticas, que permitan la generación de copias de la información de manera total e incremental.

B.2. El responsable del etiquetado físico del respaldo deberá incluir en la etiqueta la fecha, tipo de respaldo y contenido del mismo.

B.3. Los respaldos generados deberán ser probados mediante pruebas de restauración con la finalidad de validar su utilización.

B.4. La información respaldada deberá ser almacenada fuera del Centro de Datos y fuera de las oficinas centrales.

B.5. Las cintas generadas de los respaldos, una vez utilizadas en su máxima capacidad, deberán ser trasladadas y almacenadas en la Unidad de Atención a Usuarios A5.

B.6. Las cintas almacenadas en la Unidad de Atención a Usuarios del Municipio de Pachuca, deberán ser custodiadas para evitar que personas ajenas a la Comisión Nacional tengan acceso a ellas.

B.7. Los respaldos deberán ser almacenados de acuerdo al tipo de información y en cumplimiento a la normatividad aplicable.

B.8. El RSI, en coordinación con los responsables de la información, deberán revisar periódicamente el cumplimiento de esta Política.

14. POLÍTICA DE GESTIÓN DE PROVEEDORES

A. Gestión de Proveedores

A.1. Deberá existir un contrato donde se establezca el objetivo y alcance del servicio, así como la relación entre las partes.

A.2. La CONDUSEF deberá notificar a los proveedores las Políticas descritas en este documento, a las cuales el proveedor deberá apegarse y dar cumplimiento.

A.3. La CONDUSEF deberá mantener un registro de los proveedores de Tecnologías de la Información con los que tenga contratados servicios, así como los permisos otorgados para cada uno.

A.4. Los proveedores deberán firmar un Acuerdo de Confidencialidad previo al inicio de cualquier proyecto. El acuerdo deberá contener, de manera enunciativa más no limitativa:

- No divulgar la información a la que tenga acceso.
- Apegarse a la normativa interna de la Comisión Nacional.
- Periodo por el cual no debe divulgar la información a la que acceda.
- Sanciones a las que podría hacerse acreedor en caso de incumplir con el acuerdo.

A.5. El proveedor deberá identificar y enlistar los activos que considere necesarios para llevar a cabo las actividades del servicio, así como el periodo necesario de utilización, para gestionar el acceso correspondiente.

A.6. La información y activos a los que los proveedores accedan, deberán estar claramente identificados por los servidores públicos de la CONDUSEF.

A.7. Los proveedores deberán hacer del conocimiento de los servidores públicos de la CONDUSEF, una lista de contactos a los que se pueda acudir para la comunicación de requerimientos, cambios y/o atención de incidentes en la entrega del servicio.

A.8. Los proveedores deberán facilitar la información que la CONDUSEF, considere necesaria para la atención de auditorías internas y/o externas.

A.9. La CONDUSEF podrá efectuar auditorías a los proveedores de servicios, en el momento que considere necesario.

A.10. Los proveedores deberán apegarse a los controles de seguridad establecidos en la CONDUSEF, para efectuar sus actividades y proteger los activos de la Comisión Nacional.

A.11. Los proveedores deberán abstenerse a compartir información, a través de canales inseguros, a personal ajeno al proyecto o servicio que se esté desarrollando.

A.12. Los proveedores de Activos de Información deberán contar con un Plan de Contingencia que garantice la continuidad de la operación, y este deberá estar en concordancia con el Plan de Recuperación de Desastres (DRP) de la CONDUSEF.

A.13. El proveedor deberá contar con el Activo de TIC necesario, para brindar atención de servicio en sitio.

VI. INCUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

A. Proveedores de Tecnologías de la Información

El incumplimiento, omisión o violación de las Políticas de Seguridad de la Información por parte de proveedores contratados por la CONDUSEF podrá dar lugar a la aplicación de sanciones contractuales, administrativas o legales, conforme a la gravedad del caso.

Toda sanción deberá estar documentada y avalada por el RSI, en coordinación con el área jurídica correspondiente.

B. Servidores públicos de la CONDUSEF

La omisión, violación o desatención a las Políticas de Seguridad de la Información por parte de las personas servidoras públicas de la CONDUSEF será considerada una falta administrativa, y será sancionada conforme a la legislación aplicable.

VII. CONSIDERACIONES GENERALES

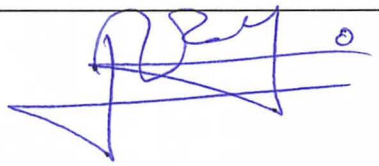
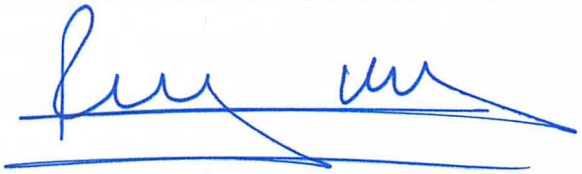
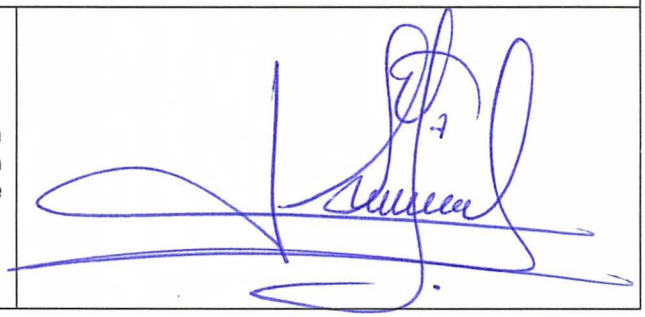
1. Las presentes Políticas están alineadas al ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las Tecnologías de la Información y Comunicación, y la seguridad de la información, en la Administración Pública Federal.

2. Las versiones posteriores a este documento se registrarán en el formato que aparece en el apartado VIII. CONTROL DEL DOCUMENTO.

VIII. CONTROL DEL DOCUMENTO

Versión	Fecha	Referencia del Cambio
1.0	15-Octubre-2019	Elaboración, firma de revisión y autorización.
2.0	04-Mayo-2021	Robustecimiento del documento para alinearse en favor de las estrategias internas de Seguridad de la Información.
3.0	21-Agosto-2022	Actualización de las Políticas de Seguridad de la Información, alineadas al Acuerdo publicado en el Diario Oficial de la Federación el 06 de septiembre de 2021.
4.0	18-Agosto-2023	Robustecimiento del documento para alinearse en favor de las estrategias internas de Seguridad de la Información.
5.0	26-Marzo-2023	Robustecimiento del documento para alinearse en favor de las estrategias internas de Seguridad de la Información.
6.0	20-Junio-2025	Robustecimiento del documento para alinearse en favor de las estrategias internas de Seguridad de la Información.

FIRMAS DE VALIDACIÓN

NOMBRE Y PUESTO	FIRMA Y RÚBRICA
· **ÁREAS RESPONSABLES**	
RICARDO BECERRIL HERRERA, Director de Tecnologías de la Información y Comunicaciones.	
CUAUHTÉMOC CARLOS JUÁREZ PÉREZ, Jefe del Departamento de Análisis e Instrumentación de la Estrategia Digital Nacional.	
· **DIRECCIÓN GENERAL DE SERVICIOS JURÍDICOS**	
RODRIGO JUVENTINO GARCÍA ISLAS LEAL, Director General de Servicios Jurídicos.	
· **DIRECCIÓN DE PLANEACIÓN Y FINANZAS**	
CITLALI MONSERRAT SERRANO GARCÍA, **Directora de Disposiciones Jurídicas.** **Designada mediante oficio VPA/301/2025, para continuar con la gestión de los asuntos de la Dirección de Planeación y Finanzas, a partir del 01 de septiembre de 2025.**	

TRANSITORIOS

PRIMERO. - Las presentes Políticas entrarán en vigor al día siguiente de su publicación en la Normateca Interna de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

SEGUNDO. - La entrada en vigor de las presentes Políticas, deja sin efectos a las **"Políticas de Seguridad de la Información"** fechadas en mayo de 2024.