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

Noviembre 2022

ÍNDICE

		PÁGINA
INTRODUCCIÓN		4
I.	ÁMBITO DE APLICACIÓN, RESPONSABLES Y OBLIGACIONES	5
II.	MARCO JURÍDICO - ADMINISTRATIVO	6
III.	DEFINICIONES Y ACRÓNIMOS	7
IV.	OBJETIVO	9
V.	PROCEDIMIENTO Y APLICACIÓN DE LAS POLÍTICAS	10
1.	POLÍTICA DE ORGANIZACIÓN INTERNA DE SEGURIDAD DE LA INFORMACIÓN	10
A.	Administración de la Seguridad de la Información	10
B.	Estructura de la Seguridad de la Información	10
C.	Cuidado y Uso de los Recursos Informáticos	11
D.	Acuerdos de Confidencialidad	13
E.	Contacto con las Autoridades	14
F.	Contacto con Organizaciones de Especial Interés	14
G.	Revisión Independiente de la Seguridad de la Información	15
H.	Tratamiento de la Seguridad en Contratos con Terceros	15
2.	POLÍTICA DE CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	18
A.	Capacitación General para Usuarios	18
B.	Concientización, Educación y Capacitación en Temas de Seguridad de la Información	19
3.	POLÍTICA PARA LA CREACIÓN DE USUARIOS Y CONTRASEÑAS	21
A.	Criterios Generales	21
B.	Criterios para la Creación de Usuarios	23
C.	Criterios para la Creación de Contraseñas	23
4.	POLÍTICA DE CONTROL DE ACCESOS	24
A.	Control de Acceso sobre Cuentas de Usuario	24
B.	Administración de Usuarios y Contraseñas	24
C.	Eliminación de Cuentas	26

D. Bloqueo y Desbloqueo de Cuentas 26
E. Revisión de Cuentas Existentes 27
F. Cuentas Nuevas 27
5. POLÍTICA DE ADMINISTRACIÓN DE OPERACIONES 28
A. Uso de Aplicaciones Institucionales con Acceso a Información Sensible 28
B. Del Correo Electrónico 28
C. Uso de Internet 29
D. Del Correcto Uso de Contraseñas 30
E. De la Protección en Lugares Públicos 30
F. Mecanismos contra Código Malicioso 31
G. Dispositivos Móviles 32
H. Servicios de Telefonía 33
I. Equipo Desatendido 33
6. POLÍTICA PARA EL DESARROLLO DE SISTEMAS INFORMÁTICOS 34
A. Del Equipo de Desarrollo 34
B. Del Administrador del Proyecto 34
C. De Todas y Todos los Involucrados 34
7. POLÍTICA DE CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN 35
A. Clasificación de la Información 35
B. Etiquetado y Confidencialidad de la Información 36
8. POLÍTICA DE GESTIÓN DE ACTIVOS 37
A. Propiedad de los Activos 37
B. Inventario de Activos 38
C. Uso Aceptable de los Activos 39
D. Uso Inapropiado de los Recursos Informáticos 39
E. Responsabilidad sobre los Activos 40
F. Devolución de los Activos 40
9. POLÍTICA DE MANEJO DE MEDIOS 41
A. Gestión de Dispositivos de Almacenamiento de Datos 41

B. Eliminación de Datos en Dispositivos de Almacenamiento Externo 42
C. Soportes Físicos en Tránsito 43
10. POLÍTICA DE BORRADO SEGURO 44
A. Dispositivos a los que se les Aplicará el Borrado Seguro 44
B. Estándares Aprobados para el Borrado Seguro 44
C. Certificación de la Herramienta 44
D. Información a Integrar en el Reporte 45
E. Excepciones 45
11. POLÍTICA DE CIFRADO DE INFORMACIÓN 46
A. Controles Criptográficos 46
B. Administración de Llaves 46
12. POLÍTICA DE SEGURIDAD FÍSICA 48
A. Mantenimiento de los Equipos 48
B. Seguridad de los Equipos Fuera de las Instalaciones 49
C. Reutilización o Retiro Seguro de los Equipos 50
13. POLÍTICA DE RESPALDOS 51
A. Sistemas, Activos y Herramientas a Respaldar 51
B. Generación de Respaldos 51
14. POLÍTICA DE GESTIÓN DE PROVEEDORES 52
A. Gestión de Proveedores 52
VI. CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES 54
VII. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 55
A. De los Proveedores de Tecnologías de la Información de la CONDUSEF 55
B. De los Servidores Públicos de la CONDUSEF 55
VIII. CONSIDERACIONES GENERALES 56
IX. CONTROL DEL DOCUMENTO 57
FIRMAS DE VALIDACIÓN 58
TRANSITORIOS 59

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 conferidas en los artículos 15, fracción III; 44, fracción XIX y 46, fracciones III, IV, V, VII y VIII, 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 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, 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.
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.
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.
Política	A la intención e instrucción global en la manera que formalmente ha sido expresada por la dirección de la Institución.
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.
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 Políticas de Seguridad de la Información que deben de seguir los servidores públicos y Terceros interesados, para mantener la Confidencialidad, integridad y disponibilidad de los activos de información de la Comisión Nacional.

V. PROCEDIMIENTO Y APLICACIÓN DE LAS POLÍTICAS

1. POLÍTICA DE ORGANIZACIÓN INTERNA DE SEGURIDAD DE LA INFORMACIÓN

A. Administración de la Seguridad de la Información

A.1. La DTIC, garantizará la correcta alineación de las acciones en materia de seguridad de la información con los requerimientos de la CONDUSEF, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos relacionados.

A.2. El Titular de la DTIC será el Responsable de la Seguridad de la información, el cual planificará, desarrollará, controlará y gestionará las políticas, procedimientos y acciones, con el fin de preservar la Seguridad de la Información dentro de sus pilares fundamentales de Confidencialidad, Integridad y Disponibilidad.

B. Estructura de la Seguridad de la Información

B.1. El Esquema de Gobierno de Seguridad de la Información establecido para gestionar todas las actividades en esta materia, se encuentra basado en roles definidos que cumplen y soportan las funciones necesarias para la administración de la Seguridad de la Información en la CONDUSEF.

B.2. El Esquema de Gobierno de Seguridad de la Información se encuentra definido en tres niveles de clasificación (estratégico, táctico y operativo), con la finalidad de determinar las responsabilidades y segregación de funciones, para una efectiva administración de Seguridad de la Información.

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. Cuidado y Uso de los Recursos Informáticos

C.1. Será responsabilidad de los Usuarios de bienes, servicios informáticos y cualquier Activo de TIC, cumplir con las Políticas de Seguridad de la Información descritos en el presente documento.

C.2. El Usuario deberá utilizar los recursos tecnológicos que tenga asignados, única y exclusivamente para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.

C.3. Al Usuario que le sean asignados recursos informáticos propiedad de la CONDUSEF será responsable de su buen uso en el desempeño de las actividades propias al cargo.

C.4. La DTIC es responsable de mantener, operar, asegurar y mejorar la infraestructura de cómputo y telecomunicaciones, con acciones que permitan otorgar los recursos informáticos necesarios para que la CONDUSEF cumpla con sus funciones.

C.5. El Usuario deberá aceptar las condiciones de uso de los recursos informáticos, a través del medio que se habilite para tal fin.

C.6. Con la finalidad de coadyuvar con el cuidado del medio ambiente, el Usuario deberá apagar los equipos de cómputo al término de su jornada laboral, a excepción de aquellos casos particulares en los que el equipo de cómputo deba permanecer en operación sin interrupción.

C.7. El Usuario deberá otorgar las facilidades necesarias para que el personal responsable de la DTIC realice los servicios de mantenimiento preventivo y correctivo a los equipos de cómputo.

C.8. Cuando un Activo de TIC presente fallas en su funcionamiento, el Usuario deberá contactar a la mesa de ayuda para que el equipo de soporte solucione el problema y evitará tratar de corregirlo por cuenta propia, esto con el fin de no comprometer la integridad del mismo.

C.9. Al finalizar la relación laboral o ante un cambio de adscripción, el Usuario deberá entregar a la DTIC, formal y materialmente los recursos informáticos asignados.

C.10. En relación a los equipos de impresión, se recomienda lo siguiente:

C.10.1. Asignar privilegios al Usuario tomando en cuenta la importancia de los documentos a imprimir, priorizando en todo momento la generación de documentos digitales, con la finalidad de forjar un ahorro en el uso de consumibles.

C.10.2. Evitar impresión de documentos para su revisión, prevaleciendo en todo momento las correcciones de manera digital.

C.10.3. Prescindir de impresiones de correos electrónicos.

C.10.4. Imprimir de preferencia en dúplex (impresión en ambos lados de la hoja).

C.10.5. Evitar las impresiones a color innecesarias, buscando priorizar la de escala monocromática.

C.10.6. Promover el uso de áreas de impresión común.

C.11. Queda estrictamente prohibido:

C.11.1. Ingerir bebidas y alimentos sobre cualquiera de los recursos informáticos, o realizar alguna actividad que puedan ponerlos en riesgo, por lo que, en caso de un daño imputable a un mal uso, el Usuario deberá realizar el trámite para resarcir el daño ante las instancias correspondientes.

C.11.2. Conectar cualquier dispositivo de red como hubs, switches, routers, access points, entre otros, así como ejecutar cualquier herramienta de monitoreo o escaneo. Lo anterior, para prevenir y evitar poner en riesgo a la red institucional de la CONDUSEF.

C.11.3. Reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno o malicioso; información confidencial o reservada propiedad de la CONDUSEF sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que puedan distraer a los servidores públicos en el desempeño de sus funciones o que comprometa la integridad de los bienes informáticos y los servicios de red.

C.11.4. Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad a través de los recursos informáticos en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la CONDUSEF.

D. Acuerdos de Confidencialidad

D.1. Se deberán establecer 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.

D.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.

D.3. Los contratos laborales de los servidores públicos con la CONDUSEF deberán contener Cláusulas de Confidencialidad.

E. Contacto con las Autoridades

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

E.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.

E.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.

F. Contacto con Organizaciones de Especial Interés

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

F.2. La participación de estos grupos deberá:

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

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

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

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

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

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

F.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.

G. Revisión Independiente de la Seguridad de la Información

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

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

G.2.1. Revisar la implementación y apego a los controles definidos para proteger la información.

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

G.2.3. Proporcionar las recomendaciones pertinentes.

G.3. Las actividades de revisión rutinarias deberán ser acordadas, planeadas y notificadas, para minimizar el riesgo de interrupciones en los procesos y servicios de la CONDUSEF.

G.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.

H. Tratamiento de la Seguridad en Contratos con Terceros

H.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:

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

H.1.2. Protección de los Activos de Información.

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

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

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

H.1.6. Obligaciones de las partes que suscriben el contrato.

H.1.7. Existencia de Derechos de Propiedad Intelectual tales como:

a. Autorización de Uso o Licenciamiento.

b. Cesión de Derechos.

c. Derecho a Actualizaciones.

H.1.8. 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.

H.1.9. 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.

H.1.10. Definición de criterios de desempeño comprobables de monitoreo y de presentación de informes.

H.1.11. Actividades de auditoría de responsabilidades contractuales o surgidas del acuerdo con Terceros.

H.1.12. Establecimiento de un proceso para la resolución de problemas y, en caso de no corresponder, disposiciones con relación a situaciones de contingencia.

H.1.13. Responsabilidades relativas a la instalación, configuración, puesta a punto y al mantenimiento de hardware y software.

H.1.14. Proceso claro y detallado de administración de cambios.

H.1.15. Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

H.1.16. Planes de entrenamiento y capacitación de Usuarios y administradores en materia de seguridad.

H.1.17. Controles que garanticen la protección contra software malicioso.

H.1.18. Elaboración y presentación de informes, notificación, investigación y estudio de incidentes y violaciones relativos a la seguridad.

H.1.19. Relación entre Terceros y subcontratistas.

H.1.20. 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.

H.1.21. 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.

H.1.22. 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.

H.1.23. 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.

2. POLÍTICA DE CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

A. Capacitación General para Usuarios

A.1. La DTIC, deberá realizar periódicamente sesiones de sensibilización a servidores públicos, considerando para ello las Políticas de Seguridad de la Información definidas, los requerimientos de seguridad de las legislaciones aplicables, tales como la LGPDPPSO, etc., así como las mejores prácticas vigentes de seguridad.

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. Concientización, Educación y Capacitación en Temas de Seguridad de la Información

B.1. El RSI, diseñará un programa de capacitación con temas de Seguridad de la Información, el cual deberá estar suscrito dentro del MGSI. Asimismo, este deberá integrarse al Programa de Capacitación Institucional de la CONDUSEF.

B.2. Para la concientización, educación y capacitación en temas de Seguridad de la Información, deberá considerarse lo siguiente:

B.2.1. Todos los servidores públicos de nuevo ingreso deberán recibir dentro de su Programa de Inducción, una presentación que contenga las políticas, procedimientos y sanciones en materia de Seguridad de la Información vigentes en CONDUSEF.

B.2.2. Deberá ser incluido en los cursos de inducción, todo aquel proveedor o Tercero que, por la naturaleza de sus funciones, labore recurrentemente (por un periodo mayor a 30 días) y tengan acceso a la información privilegiada y confidencial y/o a las instalaciones de CONDUSEF.

B.2.3. Todo servidor público de CONDUSEF deberá recibir información y/o capacitación periódica que lo concientice sobre temas y problemas de Seguridad de la Información.

B.2.4. La CONDUSEF, deberá contar con los métodos indicados que permitan reforzar la cultura de seguridad en los servidores públicos, como:

1) Correo Electrónico.
2) Promover Videos Informativos.
3) Promover Pláticas de Seguridad de la Información.
4) Curso de Capacitación (presencial o en línea).

B.2.5. 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.3. Los resultados de la capacitación deberán ser exitosos para 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.4. La DTIC, deberá asumir las siguientes responsabilidades:

B.4.1. 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.4.2. Brindarles los recursos para que conozcan las Políticas de Seguridad de la Información.

B.4.3. Motivarlos constantemente para cumplir cabalmente con las Políticas de Seguridad de la Información.

B.4.4. Brindar las facilidades para que participen en los programas de concientización relativos a la Seguridad de la Información.

B.5. Los servidores públicos, contratistas 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.6. 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.

3. POLÍTICA PARA LA CREACIÓN DE USUARIOS Y CONTRASEÑAS

A. Criterios Generales

A.1. La asignación de acceso a la información, deberá cumplir con los privilegios de Usuario y contar siempre con una justificación laboral y aprobaciones adecuadas.

A.2. Cada Usuario será responsable de la cuenta de acceso 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 identificador de Usuario, por lo cual, deberán abstenerse de divulgar su identificador a Terceros, así como de utilizar identificadores 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 mensajería electrónica, 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.6.2. 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 mencionar y teclear contraseñas en frente de otros.

A.8. Será responsabilidad de cada Usuario 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 evitarán activar o hacer uso de la opción de recordar contraseña o recordar credenciales de acceso a las aplicaciones.

A.11. No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado por la DTIC deberá ser único 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 Responsable de la Unidad Administrativa de que se trate.

B. Criterios para la Creación de Usuarios

B.1. Para efectos de las presentes Políticas, se definen dos tipos de cuentas de Usuario:

a) **Cuenta de Usuario de Sistema de Información**: Todas aquellas cuentas que sean utilizadas por los Usuarios para acceder a los diferentes Sistemas de Información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de Usuario del Sistema.

b) **Cuenta de Administración de Sistema de Información**: Corresponde a la cuenta de Usuario que permite al Administrador del Sistema realizar tareas específicas de Usuario a nivel directivo como, por ejemplo: agregar/modificar/eliminar cuentas de Usuario del Sistema.

C. Criterios para la Creación de Contraseñas

C.1. Una contraseña segura deberá cumplir con las siguientes características:

C.1.1. La longitud debe ser al menos de 8 caracteres.

C.1.2. Estar compuesta por al menos 1 caracter de los siguientes grupos:

- Letras mayúsculas
- Letras minúsculas
- Números
- Caracteres especiales (_, -, /, *, $, ¡, ¿, =, +, etc.)
- No deberá ser una palabra por sí sola, en ningún lenguaje, dialecto, jerga, etc.
- No deberá ser un palíndromo (ejemplo: agasaga)

- No deberá ser basada en información personal, nombres de familia, fechas de nacimiento, nombres de mascotas, etc.
- No deberá coincidir con alguna de las últimas 2 contraseñas utilizadas.

4. POLÍTICA DE CONTROL DE ACCESOS

A. Control de Acceso sobre Cuentas de Usuario

A.1. El identificador del Usuario (user-id) deberá ser único por cada Sistema de Información o equipo de cómputo, salvo aquellos casos en donde exista una autenticación centralizada, por ejemplo, Active Directory. En un mismo Sistema no pueden existir dos cuentas iguales.

A.2. Las cuentas de Usuario para recursos de cómputo deberán ser utilizadas sólo por el Usuario a quien fueron asignadas; por lo tanto, quedará estrictamente prohibido el uso compartido de cuentas de Usuario y contraseña o de lo contrario la persona responsable del acceso se hará acreedora a las sanciones correspondientes.

A.3. Se evitará el activar o hacer uso de la utilidad de recordar contraseña, o recordar la contraseña de las aplicaciones. Podrá utilizarse algún administrador de contraseñas que cuente con la aprobación del grupo de seguridad.

A.4. En el caso de contraseñas de acceso remoto, el Usuario deberá asegurarse que el Usuario y password que utilice en un equipo de cómputo ajeno, no se quede guardado o registrado en la memoria del navegador o sistema operativo del ordenador utilizado.

B. Administración de Usuarios y Contraseñas

B.1. El Administrador de Usuarios deberá efectuar el alta o registro de una nueva cuenta de Usuario con su respectivo perfil a los Sistemas de Información, servicios de información o acceso a la infraestructura tecnológica propiedad de la CONDUSEF, de acuerdo a los protocolos de seguridad de encriptación correspondientes.

B.2. Las cuentas de Usuario final deberán ser restringidas o limitadas a las funciones, roles o perfiles del Usuario y en ningún caso, el Usuario final podrá tener una cuenta con privilegios de administrador, a excepción de aquellas que han sido solicitadas por escrito por algún funcionario con la jerarquía suficiente y justificación correspondiente; cuando así ocurra deberá documentarse rigurosamente.

B.3. El administrador de un recurso de procesamiento de información, deberá llevar un registro de las cuentas que ha creado para conceder permisos para originar, modificar o borrar información específica. Deberá estar integrado en cada activo que cuente con un método de acceso, estos registros deberán ser documentados y controlados.

B.4. Al término de la relación laboral del servidor público con la CONDUSEF, se inhabilitarán o darán de baja de forma inmediata las cuentas de Usuario correspondientes. La información del Usuario permanecerá almacenada temporalmente, salvo aquellos casos que, por disposición legal, tengan que preservarse cierto tiempo, y podrá ser solicitada por el Titular del área de acuerdo a las Políticas definidas.

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 e-mail, sólo los niveles de permisos mínimos necesarios para el cumplimiento de sus actividades cotidianas.

C. Eliminación de Cuentas

C.1. Las cuentas de Usuario deberán ser eliminadas cuando se presente alguna de las situaciones siguientes:

C.1.1. Terminación de la relación laboral.

C.1.2. Terminación de la función para la cual fue creada la cuenta del Usuario.

C.1.3. Inactividad de la cuenta de Usuario en un periodo de 45 días naturales, será motivo para la inhabilitación (No eliminación).

Después de 90 días naturales de inactividad, se procederá a su eliminación y únicamente se generará un respaldo en los casos que cuenten con una razón definida que lo justifique.

C.2. El administrador del área responsable de la asignación de cuentas de Usuario y contraseñas, deberá eliminar o reasignar cualquier cuenta de Usuario que haya cambiado de situación laboral, o haya causado baja en la CONDUSEF.

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.

D. Bloqueo y Desbloqueo de Cuentas

D.1. Las cuentas podrán ser bloqueadas bajo los siguientes criterios:

D.1.1. Al realizar el Usuario 3 intentos fallidos de acceso.

D.1.2. Si está inactiva por 45 días naturales.

En caso de existir excepciones deberán ser justificadas y aprobadas por la DTIC.

D.1.3. Si se encuentra involucrada en un Incidente de Seguridad.

D.2. Las cuentas bloqueadas sólo podrán ser reactivadas por la DTIC, con la aprobación del mando inmediato superior del Usuario afectado.

D.3. El administrador del área responsable de la asignación de cuentas de Usuario y contraseñas, o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas, deberán bloquear cualquier cuenta de Usuario que no se haya firmado en el sistema o la red después de 45 días.

E. Revisión de Cuentas Existentes

E.1. La DTIC, en conjunto con los responsables de la información, deberán revisar periódicamente las cuentas existentes y los privilegios respectivos del Usuario final, de un grupo de Usuarios de servicio y proveedores o invitados. Deberá realizarse una auditoría cada 45 días como mínimo.

E.2. 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.

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 el jefe inmediato autorizando el alta y el Usuario aceptando las 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

A. Uso de Aplicaciones Institucionales con Acceso a Información Sensible

A.1. Cuando se requiera el acceso de un aplicativo institucional con acceso a información sensible o un acceso o consulta de información directa de las bases de datos, este deberá solicitarse formalmente a la DTIC por medio de un escrito por parte del Responsable de la Unidad Administrativa de que se trate.

A.2. Será responsabilidad de los administradores de los Sistemas Institucionales con acceso a información reservada, sensible o confidencial, depurar semestralmente el Catálogo de Cuentas de Usuarios y llevar una bitácora de las altas, bajas y cambios en tales cuentas.

B. Del Correo Electrónico

B.1. Toda cuenta de correo electrónico asignada a las Unidades Administrativas de la CONDUSEF, deberá tener asignado al servidor público responsable de la misma.

B.2. Los Usuarios deberán de abstenerse de usar cuentas de correo electrónico asignadas a otras personas, así como de recibir mensajes en cuentas de otros.

B.3. 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.

B.4. La CONDUSEF se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico del personal que ha comprometido la seguridad, violado criterios de Seguridad Informática de esta Comisión Nacional o realizado acciones no autorizadas.

B.5. El Usuario deberá utilizar el correo electrónico de la CONDUSEF que tenga asignado, única y exclusivamente para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso, así como para fines personales y/o comerciales.

B.6. 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 publicación 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.

C. Uso de Internet

C.1. El acceso a Internet provisto a los Usuarios de la CONDUSEF es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

C.2. 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.

C.3. Se considerará que los Usuarios de Internet de la CONDUSEF, tienen conocimiento y aceptan que:

C.3.1. Toda actividad realizada con el servicio de navegación en Internet será de única responsabilidad del Usuario.

C.3.2. Se prohíbe el acceso a los sitios o páginas web que contengan materiales pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano; para el caso de sitios, redes sociales, blogs, web de comentarios y páginas de intercambio de archivos que sean catalogadas como una amenaza a la Seguridad de la Información, deberán solicitar la autorización para su acceso a la DTIC, debiendo justificar debidamente que es necesario para el desarrollo de sus funciones, quedando a criterio de la DTIC la resolución que se dé al respecto.

C.3.3. Serán sujetos de monitoreo de las actividades que realiza en los sitios en Internet.

C.3.4. Se monitoree el consumo de ancho de banda en sus navegaciones por Internet.

C.3.5. Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.

C.3.6. Se prohíbe la descarga de software sin la autorización de la DTIC.

C.3.7. La utilización de Internet será para el desempeño de su función y puesto en la CONDUSEF y no para propósitos personales.

C.4. Queda estrictamente prohibido el uso de redes sociales, a excepción de aquellos servidores públicos que por sus funciones así lo requieran (sin que este beneficio se traduzca en un uso indebido), esto debido a que pueden vulnerar la seguridad por redirección a sitios web o descarga de contenidos acompañados de amenazas informáticas como códigos maliciosos.

D. Del Correcto Uso de Contraseñas

D.1. Los Usuarios, para el correcto uso de contraseñas deberán apegarse a las Políticas de contraseñas emitidas en este mismo documento.

D.2. El Usuario protegerá todos los equipos que utilice con contraseña, autenticación de varios factores, y para el caso de los móviles identificación de huella digital. No compartirá sus contraseñas con nadie.

D.3. Cada Usuario deberá reportar a la DTIC, a través de la mesa de ayuda, cualquier Incidente de Seguridad relacionado con sus datos de identificación y autenticación (Usuario y contraseña), o cuando sospeche que esta información ha sido comprometida.

D.4. Cuando se asigne o restablezca una contraseña, ésta deberá ser temporal y cambiarse en el primer uso.

E. De la Protección en Lugares Públicos

E.1. Cuando se tenga la necesidad de acceder en lugares públicos, siempre deberá cerrar sesión en las computadoras de uso público, en particular si ingresó a su correo electrónico. Además, nunca deberá marcar la opción "recordar" Usuario y contraseña en los navegadores. Siempre se deberá utilizar un inicio de sesión seguro con https:// si está disponible.

E.2. Al conectarse a redes en lugares públicos lo más seguro es usar una conexión 3G o 4G en lugar de redes Wi-Fi públicas. Desactivar la conexión Wi-Fi cuando no se esté utilizando, habilitar el cortafuegos y desactivar la detección de redes.

E.3. Si el Usuario por la naturaleza de su trabajo 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.

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 interno, 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 de la CONDUSEF 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, empleado 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 de la CONDUSEF 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 función 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 en la CONDUSEF, y así mismo por que 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 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 Sistemas 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 DE SISTEMAS INFORMÁTICOS

A. Del Equipo de Desarrollo

A.1. El equipo de desarrollo deberá evitar cualquier práctica que pueda derivar en riesgos para el Sistema Informático, citando como ejemplos de manera enunciativa más no limitativa:

A.1.1. Creación de mecanismos de puerta trasera.

A.1.2. Incorporación de Usuarios y/o claves de acceso en el código fuente.

A.1.3. Libre conformación de consultas a bases de datos a partir de entradas de Usuario.

A.1.4. Exposición de código ejecutable que revele aspectos internos en el lado del cliente.

A.1.5. Almacenamiento en medios o la transmisión de información en red de manera no controlada; entre otros.

B. Del Administrador del Proyecto

B.1. El Administrador del Proyecto deberá asegurarse que el Sistema Informático se apegue a los niveles de seguridad de acceso a la información y al sistema, de acuerdo a las facultades o roles de cada Usuario.

C. De Todas y Todos los Involucrados

C.1. Para todas y todos los Usuarios involucrados en el Desarrollo del Sistema, deberán evitar prácticas que pongan en riesgo la Confidencialidad, Integridad y Disponibilidad de la Información en cualquiera de las etapas del Proyecto.

C.2. Cualquier Sistema Informático que tenga funciones de servidor o que preste servicios a más de un Usuario, a la vez, por instancia, deberá implantarse en el ambiente de producción definido por la DTIC.

7. POLÍTICA DE CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

A. Clasificación de la Información

A.1. Se deberán definir y establecer los criterios de Clasificación de la Información, con el objeto de delimitar los casos en que sea del dominio público, "restringida" o "confidencial", incluyendo los datos personales, los cuales quedarán sujetos a la normativa establecida para tal efecto (leyes, reglamentos y otras disposiciones en materia de protección de datos personales).

A.2. La CONDUSEF será la encargada de expedir a través del RSI, criterios específicos de clasificación y etiquetado de la información.

A.3. Se deberán establecer las medidas necesarias de seguridad en el tratamiento de la información, que prevengan las fugas de ésta y permitan su detección oportuna.

A.4. La CONDUSEF deberá llevar a cabo la Clasificación de la Información en el momento en que:

A.4.1. Se genere, obtenga, adquiera o transforme la información, o

A.4.2. Se reciba una solicitud de acceso a la información, en el caso de documentos que no se hubieran clasificado previamente.

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. Etiquetado y Confidencialidad de la Información

B.1. Los documentos propiedad de la CONDUSEF que no estén clasificados como "restringidos o confidenciales" de forma clara y explícita, serán de uso y dominio público.

B.2. La CONDUSEF prohíbe a sus colaboradores el divulgar la información "restringida, confidencial, interna o pública", que pudieran obtener o manejar a través del acceso a sistemas o aplicaciones, mediante su contraseña de acceso.

B.3. Se describirán las acciones a seguir para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido, los cuales contemplarán los recursos de información en formatos físicos y electrónicos, e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión por correo, fax o correo electrónico.
- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.).

8. POLÍTICA DE GESTIÓN DE ACTIVOS

A. Propiedad de los Activos

A.1. Toda información y/o datos que se encuentren en dispositivos de almacenamiento, procesamiento, consulta, comunicaciones, transmisión, o que se gestionen en medios de comunicación, forman parte de los Activos de Información.

Lo anterior aplica para casos específicos como son:

A.1.1. Dispositivos de almacenamiento, procesamiento y/o consulta de información de datos.

A.1.2. Dispositivos de comunicaciones de datos.

A.1.3. Dispositivos de seguridad y protección de la información.

A.1.4. Medios portátiles de almacenamiento de información.

A.1.5. Dispositivos móviles.

A.1.6. Medios impresos.

A.1.7. Código de software, programas, rutinas, subrutinas, módulos, métodos, clases, algoritmos, funciones, procedimientos almacenados, disparadores, configuraciones o cualquier otra forma de código, que forme parte de un software, sistema o servicio de información.

A.2. Se considera también propiedad de CONDUSEF toda la información y datos creados, transformados, actualizados y/o mantenidos por personal interno, por clientes y/o Terceros.

Lo anterior en total independencia de quién es el propietario de equipos, dispositivos, servidores, computadoras, impresoras, medios de comunicaciones, de transmisiones, sistemas de bases de datos, licenciamiento de hardware y/o software, configuraciones, cambios o cualquier otro medio o dispositivo donde se almacene, procese o consulte la información.

A.3. 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.4. 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.5. 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.6. 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. Inventario de Activos

B.1. Se deberá lograr y mantener la protección apropiada de los activos, por lo que estos deberán ser identificados y documentados.

B.2. Se deberán de tener identificados todos los Activos de Información con los que la CONDUSEF cuenta, incluyendo todos los servicios de Tecnologías de la Información y Comunicaciones que soportan la operación diaria de esta Comisión Nacional.

B.3. El Inventario de Activos incluirá el tipo de activo, localización, información sobre licenciamiento (en caso de aplicar), fechas y registros de movimientos, proyecto o área.

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. Uso Aceptable de los Activos

C.1. El uso aceptable de los Activos de Información implica que deberán ser empleados para actividades exclusivas relacionadas con los objetivos, funciones y responsabilidades encomendadas por la CONDUSEF.

C.2. Únicamente el personal autorizado por la DTIC podrá llevar a cabo los servicios y reparaciones del equipo informático y de telefonía, por lo que los Usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

D. Uso Inapropiado de los Recursos Informáticos

D.1. Los Usuarios de la infraestructura informática de la CONDUSEF, deberán sujetarse a las restricciones aplicables durante el cumplimiento de sus responsabilidades laborales, por lo tanto, el uso inapropiado de los recursos informáticos asignados será motivo para que los servidores públicos autorizados de la DTIC puedan inhabilitar el acceso al Usuario para evitar la interrupción o daños a los servicios de información.

Las siguientes actividades se consideran como uso inapropiado de los recursos informáticos:

D.1.1. La descarga de archivos o contenido que pueda vulnerar la seguridad, debido a que vienen acompañados de amenazas informáticas como códigos maliciosos.

D.1.2. La instalación de software sin el licenciamiento necesario y/o autorizado o con fines personales, el cual puede venir acompañado de códigos maliciosos.

D.1.3. La navegación web en portales donde la consulta en estos no justifica la sustracción de información útil para las funciones del Usuario; y, asimismo, pueda generar amenazas informáticas como virus de secuencia de comandos web, troyanos, malware, etc.

D.1.4. La apertura de correo electrónico del cual se conozca una advertencia de peligro, ya sea por alerta institucional o por conocimiento público, el cual puede contener amenazas informáticas como códigos maliciosos.

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, contratistas 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, contratistas o terceras partes; así mismo, deberá cerciorarse de la completa devolución de todo el equipo.

9. POLÍTICA DE MANEJO DE MEDIOS

A. Gestión de Dispositivos de Almacenamiento de Datos

A.1. Evitar o reducir al mínimo necesario el uso de memorias USB o cualquier dispositivo portátil, para compartir o almacenar información de la CONDUSEF, en especial si contiene datos personales y/o financieros.

A.2. Las memorias USB o cualquier dispositivo de almacenamiento portátil que sea usado en equipos de cómputo de la CONDUSEF, no deberán ser conectadas en equipos de uso público o equipos de origen desconocido.

A.3. No conectar a los equipos de cómputo de la CONDUSEF, memorias USB o cualquier otro dispositivo de almacenamiento portátil que haya sido encontrado abandonado o del que no se conozca el origen.

A.4. En memorias USB o cualquier otro dispositivo de almacenamiento portátil, estará prohibido extraer de las instalaciones de la CONDUSEF, información que contenga datos personales sensibles, financieros, patrimoniales o clasificada como confidencial.

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 sensibles, financieros, patrimoniales o clasificada como confidencial 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. Eliminación de Datos en Dispositivos de Almacenamiento Externo

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

B.2. No se permitirá por ningún motivo el reciclar cintas, discos o cualquier dispositivo de almacenamiento magnético, cuando se almacene previamente información con alto nivel de clasificación.

B.3. Cuando la información está contenida en papel, ésta deberá ser destruida, de modo que la información impresa sea ilegible e irrecuperable.

B.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.

C. Soportes Físicos en Tránsito

C.1. La transmisión de la información por medios físicos requiere de los siguientes controles:

C.1.1. La información deberá ser liberada exclusivamente a las personas autorizadas definidas por el propietario de la información.

C.1.2. 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.

10. POLÍTICA DE BORRADO SEGURO

A. Dispositivos a los que se les Aplicará el Borrado Seguro

A.1. Para los discos duros de los elementos de infraestructura de servidores y almacenamiento que formen parte de la solución del proveedor, que durante la vida del contrato lleguen a tener alguna falla y que requiera la ejecución de un cambio físico y/o retiro de la infraestructura, al término del contrato, el proveedor realizará el borrado seguro de la información de la totalidad de los discos duros de los servidores y almacenamiento que forman parte de la infraestructura del servicio, mediante una herramienta y procedimiento que cumplan con los estándares internacionales, entregando a la CONDUSEF el certificado del borrado seguro.

B. Estándares Aprobados para el Borrado Seguro

B.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)

C. Certificación de la Herramienta

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

- NSTL
- OTAN
- COMMON CRITERIA

D. Información a Integrar en el Reporte

D.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.

E. Excepciones

E.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 CIFRADO DE INFORMACIÓN

A. Controles Criptográficos

A.1. Todo Usuario que utiliza y administra documentos en formato digital con información relevante de la CONDUSEF, deberá cifrar la misma de acuerdo con los requerimientos definidos por la Comisión Nacional, y de acuerdo con los niveles de Clasificación de la Información.

A.2. La información cifrada deberá utilizar como mínimo un algoritmo de cifrado mayor número de "bits" (AES de 128 comercialmente). En caso de que los Sistemas de Información no soporten dicho algoritmo, la DTIC revisará y aprobará el método de cifrado más adecuado.

A.3. Las comunicaciones a través de la red deberán utilizar un protocolo seguro para el servicio de las conexiones remotas que den acceso a la red y a los servicios de Tecnologías de la Información y Comunicaciones Institucionales, tanto para Usuarios internos como a proveedores. En caso de que los dispositivos no soporten dicho protocolo, la DTIC definirá los parámetros de seguridad que se adoptarán para el cifrado de las comunicaciones.

A.4. La transferencia de información clasificada como privilegiada y confidencial, vía correo electrónico, deberá ser cifrada por el mecanismo que haya establecido la DTIC.

A.5. La Información reservada y confidencial que sea enviada, a través de una red pública, deberá ser cifrada con el método aprobado por la DTIC, a excepción de la información que por necesidades del socio de negocio deba ser enviada sin tomar en cuenta estos controles.

A.6. Se deberá exigir a los proveedores el cifrado en la transferencia de la información o almacenamiento de la información, siempre y cuando la información que manejen se encuentre clasificada como reservada y/o confidencial.

B. Administración de Llaves

B.1. La DTIC verificará que las llaves criptográficas generadas para los sistemas criptográficos, y las diferentes aplicaciones sean protegidas contra modificaciones, pérdidas y destrucción.

B.2. Si las llaves de cifrado son enviadas por algún medio de comunicación, esto deberá hacerse en forma cifrada (cuando aplique).

B.3. Siempre que se utilice cifrado, las llaves y los métodos utilizados para generarlas deberán permanecer protegidos, y su cuidado deberá continuar mientras la información permanezca cifrada con esa llave. En caso de que la información pueda verse comprometida (por ejemplo, cambio o baja de servidores públicos que custodian las llaves, accesos no autorizados a las llaves etc.) la llave deberá ser reemplazada o actualizada de manera inmediata.

B.4. Las llaves de cifrado deberán ser divididas (cuando aplique), y cada parte deberá estar custodiada por una persona distinta; el almacenamiento de las llaves en formato de texto deberá hacerse de forma cifrada.

B.5. Si los datos en un medio de almacenamiento se encuentran cifrados, incluso en modo de respaldo, las llaves de cifrado deberán ser almacenadas en otro medio de almacenamiento separado (cuando aplique).

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.

12. POLÍTICA DE SEGURIDAD FÍSICA

A. Mantenimiento de los Equipos

A.1. Deberá efectuarse periódicamente el mantenimiento lógico preventivo de todos los equipos de cómputo y comunicación.

A.2. Para el caso de los mantenimientos preventivos lógicos, se realizará la notificación de los periodos programados, con la finalidad de que se lleven a cabo las acciones pertinentes.

A.3. Todos los equipos que albergan Sistemas de Información utilizados en el proceso de producción, deberán conservarse de acuerdo con las especificaciones e intervalos de servicio recomendados por el fabricante, realizando reparaciones y servicios ejecutados solamente por servidores públicos calificados y autorizados.

A.4. Los niveles de temperatura y humedad relativa en el Centro de Cómputo, deberán ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo instalada, para lo cual se debe utilizar un sistema de enfriamiento (aire acondicionado) acorde a las necesidades de operación.

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. Seguridad de los Equipos Fuera de las Instalaciones

B.1. El uso de los equipos fuera de las instalaciones de la CONDUSEF, deberá ser debidamente autorizado.

B.2. Se deberán aplicar las medidas de seguridad a los equipos situados fuera de las instalaciones y equipos móviles que se conectan a la red de la CONDUSEF.

B.3. Se deberá contar con un inventario de todos los equipos propiedad de la CONDUSEF, y de los equipos subarrendados, que se encuentren situados fuera y dentro de las instalaciones de la Comisión Nacional.

B.4. Se deberán determinar controles para el trabajo fuera de las instalaciones.

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. Reutilización o Retiro Seguro de los Equipos

C.1. Con la finalidad de reutilizar o retirar de forma segura los equipos, se aplicará el borrado seguro de la información.

C.2. Los equipos de cómputo y/o telecomunicaciones de las oficinas de la CONDUSEF, no deberán ser trasladados o reubicados sin la previa autorización y conocimiento del responsable correspondiente.

C.3. Para el retiro de los equipos de cómputo y/o telecomunicaciones de los inmuebles, dichos equipos deberán registrarse en una bitácora en la recepción del edificio para la entrada o salida de este.

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 y/o anexos 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. CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

La existencia de las presentes Políticas, incluyen procedimientos que dan cumplimiento a lo establecido en la normatividad vigente aplicable para la CONDUSEF, así como a lo establecido de manera contractual con los diferentes proveedores de servicios.

VII. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A. De los Proveedores de Tecnologías de la Información de la CONDUSEF

A.1. La violación, desatento u omisión de la Política para la gestión de proveedores de la CONDUSEF, generará sanciones estipuladas y avaladas, de forma escrita por el RSI, las cuales serán aplicadas de acuerdo con el grado de incumplimiento de las Políticas, hasta la rescisión contractual.

B. De los Servidores Públicos de la CONDUSEF

B.1. La violación, desatento u omisión de las Políticas de Seguridad de la Información de la CONDUSEF, generarán sanciones estipuladas y avaladas de forma escrita por el RSI, las cuales serán aplicadas de acuerdo con el grado de incumplimiento de las Políticas, hasta la rescisión laboral.

VIII. 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 IX. CONTROL DEL DOCUMENTO.

IX. 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.

FIRMAS DE VALIDACIÓN

NOMBRE Y PUESTO	FIRMA Y RÚBRICA
· **ÁREAS RESPONSABLES**	
RICARDO BECERRIL HERRERA, Director de Tecnologías de la Información y Comunicaciones.	
RAÚL LAZCANO SÁNCHEZ, Jefe de Departamento de Análisis e Instrumentación de la Estrategia Digital Nacional.	
· **DIRECCIÓN GENERAL DE SERVICIOS LEGALES**	
RODRIGO JUVENTINO GARCÍA ISLAS LEAL, Director General de Servicios Legales.	
· **DIRECCIÓN DE PLANEACIÓN Y FINANZAS**	
BERNARDITA GLORIA ARANGO FERNÁNDEZ, Directora de Planeación y Finanzas.	

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 septiembre de 2021.