



INSTITUTO DEL FONDO NACIONAL PARA EL
CONSUMO DE LOS TRABAJADORES

**MARCO DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN DEL INSTITUTO FONACOT**

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

HOJA DE AUTORIZACIÓN

ELABORÓ

Responsable de Seguridad de la Información

REVISÓ

Subdirección General de Tecnologías de la Información y
Comunicación

Dirección de Tecnologías de la Información

Dirección de Infraestructura Tecnológica

Dirección de Desarrollo de Sistemas


APROBACIÓN

El presente documento cuenta con la opinión favorable del Comité de Mejora Regulatoria Interna bajo el Acuerdo No. COM-220-120624 en su tercera sesión extraordinaria celebrada el día 12 de junio de 2024. Asimismo, fue presentado para su aprobación ante el H. Consejo Directivo en su nonagésima séptima sesión ordinaria de fecha 25 de julio de 2024, bajo el Acuerdo No. CD ME 39 - 250724.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

ÍNDICE

INTRODUCCIÓN.....	5
I. PROPÓSITO DEL MGSÍ.....	5
II. ALCANCE.....	5
III. TABLA DE CONTROL DE CAMBIOS.....	6
IV. MISIÓN Y VISIÓN DEL INSTITUTO FONACOT.....	6
V. MARCO JURÍDICO ADMINISTRATIVO.....	6
VI. CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO FONACOT.....	9
VII. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.....	10
VIII. DETERMINACIÓN DE LOS PROCESOS CRÍTICOS DEL INSTITUTO FONACOT.....	11
IX. DETERMINACIÓN DE LA CLASIFICACIÓN DE ACTIVOS.....	12
X. DETERMINACIÓN DEL ANÁLISIS DE RIESGO.....	13
XI. DETERMINACIÓN PARA LA GESTIÓN DE INCIDENTES.....	14
XII. DETERMINACIÓN PARA LA GESTIÓN DE VULNERABILIDADES.....	22
XIII. SEGURIDAD DE LA INFORMACIÓN EN LA TRANSICIÓN DEL IPV4 A IPV6.....	23
XIV. DETERMINACIÓN DE LA EVALUACIÓN Y MEJORA CONTINUA DE LOS ESTÁNDARES TÉCNICOS.....	23
XV. MEJORA CONTINUA.....	23
XVI. DETERMINACIÓN DE POLÍTICAS, PROCEDIMIENTOS, METODOLOGÍAS Y ANEXOS DE SEGURIDAD DE LA INFORMACIÓN.....	23
1. POLÍTICA DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN.....	24
2. POLÍTICA DE CONTROL DE ACCESOS.....	27
3. POLÍTICA DE CRIPTOGRAFÍA.....	36
4. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES.....	39
5. POLÍTICA DE DESARROLLO SEGURO.....	43
6. POLÍTICA DE RELACIÓN CON TERCEROS.....	49
7. POLÍTICA DE SEGURIDAD EN LAS OPERACIONES.....	52
8. POLÍTICA DE PROTECCIÓN CONTRA CIBERAMENAZAS.....	59
9. POLÍTICA DE CUMPLIMIENTO.....	60
10. POLÍTICA DE SEGURIDAD EN LOS RECURSOS HUMANOS.....	62
11. POLÍTICA DE PANTALLA Y ESCRITORIO SEGURO.....	65
12. POLÍTICA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	66
13. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	70
14. POLÍTICA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO.....	74
15. POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN.....	77
16. POLÍTICA DE USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPO DE CÓMPUTO.....	81
17. POLÍTICA DE ACCESO CON CUENTA PRIVILEGIADA.....	82
18. POLÍTICA DE CONEXIONES VPN (RED PRIVADA VIRTUAL) CLIENTE – SERVIDOR.....	84

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

19. POLÍTICA DE CORREO ELECTRÓNICO.....	85
20. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN BASES DE DATOS.....	86
21. POLÍTICA DE CONTROL DE SEGUIMIENTO A VULNERABILIDADES.....	90
22. POLÍTICA DE PLANIFICACIÓN DE RESPUESTA ANTE UNA CAUSA DE FUERZA MAYOR O DE CASO FORTUITO.....	92
23. POLÍTICA DE ASIGNACIÓN DE EQUIPO DE CÓMPUTO.....	94
24. POLÍTICA DE BORRADO SEGURO.....	97
25. POLÍTICA DE GESTIÓN DE PARCHES DE SISTEMAS OPERATIVOS.....	99
26. POLÍTICA DE NAVEGACIÓN SEGURA.....	100
27. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE SISTEMAS OPERATIVOS.....	102
28. POLÍTICA DE GESTIÓN DE INCIDENTES CIBERNÉTICOS.....	103
29. POLÍTICA DE SOLICITUD DE DESBLOQUEO DE CUENTA Y REINICIO DE CONTRASEÑA.....	105
30. POLÍTICA DE EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS TECNOLÓGICOS.....	106
31. PROCEDIMIENTO ACCIONES CORRECTIVAS Y OPORTUNIDADES DE MEJORA.....	107
32. PROCEDIMIENTO PARA HABILITAR/DESHABILITAR EL USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPOS DE CÓMPUTO.....	109
33. PROCEDIMIENTO DE GESTIÓN DE CUENTAS.....	111
34. PROCEDIMIENTO DE CONTRASEÑAS.....	114
35. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	115
36. PROCEDIMIENTO DE DESARROLLO SEGURO.....	123
37. PROCEDIMIENTO DE INSTALACIÓN DE PARCHES EN BASES DE DATOS.....	128
38. PROCEDIMIENTO DE CONTROL DE SEGUIMIENTO A VULNERABILIDADES.....	131
39. PROCEDIMIENTO DE POLÍTICAS DE COMUNICACIÓN.....	134
40. PROCEDIMIENTO PARA LA RECEPCIÓN Y ATENCIÓN DE TICKETS DE SEGURIDAD DE LA INFORMACIÓN.....	137
41. PROTOCOLO DE ATENCIÓN AL FRAUDE DE CLIENTES DEL INSTITUTO FONACOT.....	140
42. METODOLOGÍA DE LA EVALUACIÓN DE RIESGOS TECNOLÓGICOS.....	142
43. OWASP – SAMM INSTITUTO FONACOT.....	152
44. METODOLOGÍA PARA EL ANÁLISIS CAUSA RAÍZ.....	157
45. OWASP VERIFICACIÓN DE SEGURIDAD EN APLICACIONES MÓVILES.....	159
XVII. GLOSARIO DE TÉRMINOS.....	165
1 DEFINICIONES.....	165
2 ACRÓNIMOS.....	172
TRANSITORIOS.....	175

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

INTRODUCCIÓN.

El Gobierno Federal ha emitido requerimientos en materia de seguridad de la información a través del 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, publicado en el D.O.F. el 06 de septiembre de 2021.

En los siguientes apartados de dicho Acuerdo, se indica que cada Institución que forme parte del Gobierno Federal deber contar con un MGSÍ.

“TÍTULO CUARTO
POLÍTICAS TECNOLÓGICAS APLICABLES A LOS PROYECTOS DE TIC Y SI.

CAPÍTULO VI
SEGURIDAD DE LA INFORMACIÓN

Artículo 75.- Las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información, alineado a la política general de SI, que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, a través de sus sistemas, aplicaciones, infraestructura y personal; dicho MGSÍ deberá contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.

La política general de seguridad de la información está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional.”

“TRANSITORIOS

NOVENO. - El MGSÍ de cada Institución deberá integrarse y remitirse a través de la Herramienta en un plazo de 120 días hábiles a partir de la publicación de este Acuerdo.”

Por lo que el Instituto FONACOT debe contar con un MGSÍ que dé cumplimiento a lo solicitado por el Gobierno Federal.

I. PROPÓSITO DEL MGSÍ.

Dar cumplimiento a los requerimientos del Gobierno Federal en materia de seguridad de la información, a través de la estructura que es requerida para este fin:

- Definición de la política general de la seguridad de la información.
- Definición de los procesos críticos.
- Definición de la clasificación de activos de información del Instituto FONACOT.
- Definición del análisis de riesgos.
- Definición para la respuesta a incidentes.
- Definición para la gestión de vulnerabilidades.
- Definición para la supervisión de la seguridad.
- Definición de políticas, procedimientos, metodologías y anexos de seguridad de la información.
- Definición de la Mejora Continua.

II. ALCANCE.

Aplica a los activos de información del Instituto FONACOT. La aplicación de este marco considera a todo el personal laboral del Instituto FONACOT, así como a todos sus proveedores de servicios.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

III. TABLA DE CONTROL DE CAMBIOS.

No. de Versión	Fecha de Modificación	Descripción de los Cambios
MA26.00	Noviembre, 2022.	Nueva creación.
MA26.01	Julio, 2024.	<ul style="list-style-type: none"> • Actualizar lo siguiente: <ul style="list-style-type: none"> ✓ Tabla de Control de Cambios. ✓ Marco Jurídico Administrativo. ✓ Objetivos de Seguridad. ✓ Política General de Seguridad de la Información. ✓ Determinación de los procesos críticos del Instituto FONACOT. ✓ Política de Relación con Terceros. ✓ Cuentas de correo electrónico de contacto con las autoridades en la Política de Gestión de Incidentes Cibernéticos. ✓ Roles y funciones. ✓ Definiciones y Acrónimos. • Elaborar la: <ul style="list-style-type: none"> ✓ Política de Solicitud de Desbloqueo de Cuenta y Reinicio de Contraseña. ✓ Política de Evaluación y Tratamiento de los Riesgos Tecnológicos. ✓ Procedimiento de Políticas de Comunicación. • Sustituir la Política de Protección Contra el Malware por la Política de Protección contra Ciberamenazas. • Incorporación de artículos transitorios (baja versión 00 y vigencia versión 01). • Revisión de lenguaje inclusivo.

IV. MISIÓN Y VISIÓN DEL INSTITUTO FONACOT.

• MISIÓN.

Apoyar a los trabajadores de centros de trabajo afiliados, al garantizar el acceso a créditos, otorgar financiamiento y promover el ahorro, para su bienestar social y el de su familia, soportado en la sustentabilidad financiera del Instituto FONACOT.

• VISIÓN.

Ser la entidad financiera líder de los trabajadores mexicanos, con una estructura sólida, eficiente y competitiva, que presta servicios de excelencia para el otorgamiento de créditos.

V. MARCO JURÍDICO ADMINISTRATIVO

A continuación, se integra una relación de los ordenamientos legales y normativas que aplican al Instituto FONACOT en materia de seguridad de la información de forma enunciativa más no limitativa:

CONSTITUCIÓN

1. Constitución Política de los Estados Unidos Mexicanos; publicada en el D.O.F. el 05 de febrero de 1917, y sus reformas.

LEYES

1. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; publicada en el D.O.F. el 04 de enero del 2000, y sus reformas.
2. Ley de Firma Electrónica Avanzada; publicada en el D.O.F. el 11 de enero de 2012, y sus reformas.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3. Ley de la Comisión Nacional Bancaria y de Valores; publicada en el D.O.F. el 28 de abril de 1995, y sus reformas.
4. Ley del Instituto del Fondo Nacional para el Consumo de los Trabajadores; publicada en el D.O.F. el 24 de abril de 2006, y sus reformas.
5. Ley Federal de Austeridad Republicana; publicada en el D.O.F. el 19 de noviembre de 2019.
6. Ley Federal de Protección a la Propiedad Industrial; publicada en el D.O.F. el 01 de julio de 2020.
7. Ley Federal del Derecho de Autor; publicada en el D.O.F. el 24 de diciembre de 1996, y sus reformas.
8. Ley Federal del Trabajo; publicada en el D.O.F. el 01 de abril de 1970, y sus reformas.
9. Ley General de Archivos; publicada en el D.O.F. el 15 de junio de 2018, y sus reformas.
10. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; publicada en el D.O.F. el 26 de enero de 2017, y sus reformas.
11. Ley General de Transparencia y Acceso a la Información Pública; publicada en el D.O.F. el 04 de mayo de 2015, y sus reformas.

DISPOSICIONES

1. Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, publicado en el D.O.F. el 04 de noviembre del 2019, y sus reformas.

CÓDIGO

1. Código de Ética de la Administración Pública Federal; publicado en el D.O.F. el 08 de febrero de 2022.

REGLAMENTOS

1. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; publicado en el D.O.F. el 28 de julio del 2010, y sus reformas.
2. Reglamento de la Ley de Firma Electrónica Avanzada; publicado en el D.O.F. el 21 de marzo de 2014.
3. Reglamento de la Ley del Instituto del Fondo Nacional para el Consumo de los Trabajadores; publicado en el D.O.F. el 30 de noviembre del 2006.
4. Reglamento de la Ley Federal de Archivos; publicado en el D.O.F. el 13 de mayo de 2014.
5. Reglamento de la Ley Federal del Derecho de Autor; publicado en el D.O.F. el 22 de mayo de 1998, y sus reformas.

DECRETOS

1. Decreto por el que se Expide el Presupuesto de Egresos de la Federación para el Ejercicio Fiscal, vigente.
2. Decreto que Establece 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; publicado en el D.O.F. el 10 de diciembre de 2012, y sus reformas.

ACUERDOS

1. 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; publicado en el D.O.F. el 06 de septiembre de 2021.
2. Acuerdo por el que se Expide la Estrategia Digital Nacional 2021-2024; publicado en el D.O.F. el 06 de septiembre de 2021.
3. Acuerdo por el que se Emiten las Disposiciones en Materias de Recursos Humanos y del Servicio Profesional de Carrera, así como el Manual Administrativo de Aplicación General en Materia de Recursos Humanos y Organización y el Manual del Servicio Profesional de Carrera; publicado en el D.O.F. el 12 de julio de 2010, y sus reformas.
4. Acuerdo por el que se Establecen las Disposiciones en Materia de Recursos Materiales y Servicios Generales y el Manual Administrativo de Aplicación General en Materia de Recursos Materiales y Servicios Generales; publicado en el D.O.F. el 16 de julio de 2010, y sus reformas.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Acuerdo por el que se Expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público; publicado en el D.O.F. el 09 de agosto de 2010, y sus reformas.
- Acuerdo por el que se establecen las Disposiciones Generales en materia de Recursos Humanos de la Administración Pública Federal; publicado en el D.O.F. el 22 de febrero de 2024 y sus reformas.

LINEAMIENTOS

- Lineamientos en materia de Austeridad Republicana de la Administración Pública Federal; publicados en el D.O.F. el 18 de septiembre de 2020.
- Lineamientos para Regular el Funcionamiento del Registro Público de Organismos Descentralizados; publicados en el D.O.F. el 23 de noviembre de 2011, y sus reformas.
- Lineamientos por los que se Establecen Medidas de Austeridad en el Gasto de Operación en las Dependencias y Entidades de la Administración Pública Federal; publicados en el D.O.F. el 22 de febrero de 2016.
- Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones públicas; publicados en el D.O.F. el 15 de abril de 2016, y sus reformas.
- Lineamientos de Protección de Datos Personales para el Sector Público; publicados en el D.O.F. el 26 de enero de 2018, y sus reformas.
- Lineamientos Técnicos Generales para la Publicación, Homologación y Estandarización de la Información de las Obligaciones Establecidas en el Título Quinto y en la Fracción IV del Artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que Deben de Difundir los Sujetos Obligados en los Portales de Internet y en la Plataforma Nacional de Transparencia; publicados en el D.O.F. el 04 de mayo de 2016, y sus reformas.
- Lineamientos Generales para la Regulación de los Procedimientos de Rendición de Cuentas de la Administración Pública Federal; publicados en el D.O.F. el 11 de julio de 2023.

PLANES

- Plan Nacional de Desarrollo 2019-2024; publicado en el D.O.F. el 12 de julio de 2019.

PROGRAMAS

- Programa Sectorial de Trabajo y Previsión Social 2020-2024; publicado en el D.O.F. el 24 de junio de 2020.
- Programa de Trabajo Institucional 2022-2024 del Instituto del Fondo Nacional para el Consumo de los Trabajadores; publicado en el D.O.F. el 28 de junio de 2022.
- Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública, 2019-2024; publicado en el D.O.F. el 30 de agosto de 2019.

ESTATUTO

- Estatuto Orgánico del Instituto del Fondo Nacional para el Consumo de los Trabajadores, publicado en el D.O.F. el 16 de enero de 2024.

PROTOCOLOS

- Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, de la Presidencia de la República, Coordinación de Estrategia Digital Nacional, Secretaría de Seguridad y Protección Ciudadana y Guardia Nacional, octubre 2021.

GUÍAS

- Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal que Emite la Coordinación de Estrategia Digital Nacional del 07 de diciembre del 2021.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

REFERENCIAS NORMATIVAS

1. Marco de Referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología (CSF NIST), Versión 1.1 del 16 de abril de 2018.

NORMATIVIDAD INTERNA APLICABLE

1. Manual de Organización General del Instituto FONACOT, vigente.
2. Código de Conducta del Instituto FONACOT, vigente.
3. Contrato Colectivo de Trabajo, vigente.
4. Estructura Orgánica y Ocupacional autorizada por el Consejo Directivo, vigente.
5. Lineamientos por el que se Establece el Proceso de Calidad Regulatoria interna en el Instituto del Fondo Nacional para el Consumo de los Trabajadores, vigente.
6. Lineamientos, Políticas y Mecanismos de Control que Establecen los Términos y Condiciones que los Sujetos Obligados Deberán Considerar al Realizar Operaciones con Valores del Instituto FONACOT, vigente.
7. Manual de Administración Integral de Riesgos del Instituto FONACOT, vigente.
8. Manual de Calidad del Instituto FONACOT, vigente.
9. Manual de Crédito del Instituto FONACOT, vigente.
10. Manual Financiero del Instituto FONACOT, vigente.
11. Manuales de Organización Específicos de las Direcciones del Instituto FONACOT, vigentes.
12. Manuales de Políticas y Procedimientos de las Direcciones del Instituto FONACOT, vigentes.
13. Modelo del Sistema de Control Interno del Instituto FONACOT, vigente.
14. Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamiento y Servicios, vigentes.
15. Políticas, Bases y Lineamientos en Materia de Obra Pública, vigentes.
16. Procedimientos Específicos de Administración del Crédito del Instituto FONACOT, vigentes.
17. Procedimientos Específicos de Originación del Crédito del Instituto FONACOT, vigentes.
18. Procedimientos Específicos de Promoción de Crédito del Instituto FONACOT, vigentes.
19. Plan de Continuidad de Negocios del Instituto FONACOT, vigente.
20. Reglamento Interior de Trabajo del Instituto FONACOT, vigente.
21. Reglamento de Pensiones, Jubilaciones y Primas de Antigüedad, vigente.

VI. CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO FONACOT.

VI.I Objetivos de Seguridad.

A continuación, se definen los objetivos de seguridad de la información en el Instituto FONACOT:

1. Cumplir anualmente con el proceso de mejora continua del MGSI a través de las fases de planeación, ejecución, revisión y mejora, logrando la eficacia y eficiencia de las prácticas de la Seguridad de la Información.
2. Reducir el impacto de las vulnerabilidades identificadas en los análisis de vulnerabilidades llevados a cabo durante el programa anual.
3. Cumplir con la ejecución en tiempo y forma de los planes de remediación que mitigan los hallazgos relacionados con las vulnerabilidades.
4. Publicación del 100% de las infografías de sensibilización planeadas en el programa anual de Cultura de la Seguridad de la Información.
5. Mantener y/o mejorar el nivel de madurez y aprobación del MGSI respecto con los reportes semestrales presentados ante la CEDN realizados a través de la herramienta HGPTIC 2.0.

VI.II Roles y Funciones.

Responsable de la Seguridad de la Información en el Instituto FONACOT.

- Dar seguimiento a la conformación del MGSI, así como a su implementación, y al cumplimiento de los controles mínimos de seguridad.
- Presentar a sus superiores jerárquicos, incluida la persona titular del Instituto FONACOT, un informe anual sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Dar aviso inmediato al CERT-MX y/o policía cibernética sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.
- Implementar un programa de evaluaciones, que contemple verificar el desempeño de los controles de seguridad y determinar acciones de mejora.
- Hacer del conocimiento del OICE en el Instituto FONACOT y/o de las autoridades competentes las irregularidades u omisiones en el cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, en su caso los proveedores y su personal laboral, obligados a su observancia.
- Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.
- Establecer y ejecutar el Programa de Cultura de Seguridad de la Información.

Equipo de Respuesta a Incidentes de Seguridad en TIC.

- Identificación y actualización de activos esenciales de información.
- Elaboración y actualización del PCN de TIC.
- Realizar la gestión y monitoreo proactivo para la gestión de incidentes.
- Contener y mitigar la amenaza.
- Recuperar los servicios esenciales.
- Identificación de indicadores de compromiso.
- Desarrollo de las actividades post-incidente que incluye entre ellas la presentación de la denuncia ante el Ministerio Público, con ayuda de las áreas pertinentes dentro del Instituto FONACOT.
- Intercambiar activamente información con el CERT-MX y/o policía cibernética.
- Establecer el mecanismo de registro de los incidentes de seguridad de la información.
- Reportar al RSI los incidentes de seguridad de la información que se presenten.
- Integrar los datos del incidente y su solución a los repositorios del Instituto FONACOT.
- Realizar las acciones de preparación, detección, respuesta y recuperación, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

El RSI y el ERISC del Instituto FONACOT, deben realizar las acciones de preparación, detección, respuesta, recuperación, actualización y mejora Institucional, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

VII. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

La política general de seguridad de la información procura los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por el Instituto FONACOT, a través de sus sistemas, aplicaciones, infraestructura y personal, para asegurar el cumplimiento de las obligaciones institucionales, regulatorias, organizacionales, operativas y de cultura de la seguridad de la información.

Esta política, es una directriz que garantiza la certidumbre de la continuidad de las operaciones y la permanencia e integridad de la información institucional.

El alcance incluye al personal y proveedores, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MGSI que se determinan en las siguientes premisas:

- Identificar los procesos y activos críticos, así como a las áreas que participan en la gestión de la seguridad de la información, a través del PCN del Instituto FONACOT.
- Minimizar el riesgo tecnológico de los procesos del Instituto FONACOT, analizando las amenazas y vulnerabilidades.
- Cumplir con los criterios de seguridad de la información aplicando controles para la confidencialidad, integridad, disponibilidad.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Proponer, mejorar e innovar tecnologías en materia de ciberseguridad.
- Proteger los activos de información, a través de controles de seguridad de la información.
- Establecer las políticas, procedimientos y controles en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en el Instituto FONACOT, a través de un programa de formación en la cultura de seguridad de la información.
- Contar con una adecuada respuesta a incidentes de seguridad de la información.
- Implementar, operar y mejorar de forma continua el MGSi, soportado en lineamientos claros, alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen los lineamientos de seguridad que soportan el MGSi del Instituto FONACOT:

- El Instituto FONACOT revisará y en su caso actualizará el MGSi, al menos una vez al año o cuando surja una necesidad antes del término de dicho periodo.
- El Instituto FONACOT protege la información generada, procesada o resguardada por los procesos de negocio y activos de información.
- El Instituto FONACOT protege la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El Instituto FONACOT protege su información de las amenazas y vulnerabilidades a las cuales está expuesta.
- El Instituto FONACOT protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Instituto FONACOT controla la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes.
- El Instituto FONACOT implementa controles de acceso a la información, sistemas y recursos de red.
- El Instituto FONACOT avala que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Instituto FONACOT lleva a cabo la mejora continua de su modelo de seguridad, a través de una adecuada gestión de los eventos de seguridad, y las debilidades asociadas con las tecnologías de la información.
- El Instituto FONACOT mantiene la disponibilidad y continuidad de su operación tecnológica.
- El Instituto FONACOT da cumplimiento a las obligaciones legales, regulatorias y contractuales establecidas relacionadas con la seguridad de la información.

VIII. DETERMINACIÓN DE LOS PROCESOS CRÍTICOS DEL INSTITUTO FONACOT.

El Instituto FONACOT a través del PCN vigente, identifica los procesos que se manejan dentro del Instituto FONACOT y los clasifica de acuerdo con su criticidad (Muy Alta, Alta, Media y Baja).

A continuación, se listan los procesos con una criticidad *Muy Alta* y *Alta*.

Número	Nombre del Proceso	Sistema	Criticidad
1	Administración de Cuentas para el Acceso al Sistema Institucional.	CREDERE	Muy Alta
2	Mesa de control.	Sistema de Crédito y CREDERE	
3	Atención de incidentes de crédito y modificación de parámetros del sistema.	CREDERE	

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Número	Nombre del Proceso	Sistema	Criticidad	
4	Elaboración de los reportes del cierre mensual de cartera.	CREDERE		
5	Generación, Validación y Publicación de la Emisión.	CREDERE		
6	Procedimiento para la Concentración y Compensación Electrónica de Fondos.	SAP y Banca electrónica de Instituciones Bancarias		
7	Dispersión de Fondos.	CREDERE, SAP y Banca Electrónica de Instituciones Bancarias		
8	Procedimiento para el uso de líneas bancarias.	SAP		
9	Información financiera.	SAP		
10	Procedimiento Específico de Registro de la Persona Trabajadora.	Sistema de Crédito y CREDERE		
11	Atención de incidentes CREDERE.	CREDERE		
12	Atención de incidentes del Sistema de Crédito.	Sistema de Crédito		
13	Alta o modificación de productos.	CREDERE		Alta
14	Emisión de Certificados Bursátiles.	SAP		
15	Balanza de Comprobación mensual.	SAP y CREDERE		
16	Elaboración y presentación de declaraciones de impuestos.	SAP y CREDERE		
17	Operación del Centro de Atención Telefónica del Instituto FONACOT.	CREDERE y Sistema de Crédito		

IX. DETERMINACIÓN DE LA CLASIFICACIÓN DE ACTIVOS.

Identificación de todos los activos esenciales que procesen, transmitan o guarden información.

Los activos se han clasificado en las siguientes categorías:

1. Datos / Información.
2. Aplicaciones (software).
3. Aplicativo móvil.
4. Equipamiento informático.
5. Soportes de información.
6. Equipamiento auxiliar.
7. Instalaciones físicas – Inmobiliario.
8. Factor humano.
9. Infraestructura esencial.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Además, se debe contemplar la información siguiente:

- Nombre de la Institución:
- Nombre del responsable del activo:
- Cargo:
- Teléfono oficina:
- Teléfono móvil:
- Correo electrónico institucional:
- Correo electrónico alterno:
- ID Activo:
- Nombre del Activo:
- Descripción: URL o direcciones IP homologadas:
- Tipo de activo:
- Nivel de criticidad:
- Nivel de impacto

La clasificación y evaluación de activos se encuentra en la metodología de la evaluación de riesgos.

X. DETERMINACIÓN DEL ANÁLISIS DE RIESGO.

El proceso de administración de riesgos tecnológicos es el siguiente:

1. Identificación de los activos y el personal que custodia (inventario de activos).
2. Valoración de los activos con base en las dimensiones de seguridad (C+I+D).
3. Identificación de las amenazas relevantes para cada activo, con base en el PCN vigente.
 - a. El Instituto FONACOT considera al menos las siguientes amenazas relacionadas con el Centro de Datos:
 - i. Desastres naturales o ambientales (Terremotos).
 - ii. Falla en los enlaces de comunicación.
 - iii. Bloqueo por manifestantes.
 - iv. Actos vandálicos y terrorismo.
 - v. Actos mal intencionados y sabotaje de personal laboral o ajeno al Instituto FONACOT.
 - vi. Ataques cibernéticos.
 - vii. Emergencia sanitaria.
 - viii. Pérdida de personal laboral clave.
 - ix. Pérdida de información sensible, necesaria para la operación.
 - x. Pérdida de los centros de cómputo.
4. Valoración de amenazas de acuerdo con:
 - a. Estimación de la probabilidad de ocurrencia de la amenaza sobre cada activo.
 - b. Estimación de la degradación que causaría la amenaza en cada dimensión (C+I+D) del activo si esta llegase a materializarse.
5. Calcular el impacto de la amenaza sobre el activo de información y esto se realiza con base al valor del activo por la degradación (*impacto = valor del activo * degradación*).
6. Calcular el nivel de riesgo, es el impacto por la probabilidad (*riesgo = Impacto * probabilidad*).
7. Identificación de la Dirección de la Unidad Administrativa responsable de los riesgos.
8. Gestionar los riesgos:
 - a. Identificar y elegir los controles.
 - b. Valorar la estimación de eficacia de los controles.
9. Realizar el informe de la evaluación de riesgos.
10. Realizar la evaluación del riesgo residual.

X.I. Tratamiento de Riesgos de Seguridad de la Información.

Como parte del proceso de análisis y evaluación se ha definido y aplicado un proceso de tratamiento de riesgos de seguridad de la información para:

1. Seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información, tomando en cuenta los resultados de la evaluación de riesgos.
2. Determinar todos los controles que sean necesarios para poner en práctica las opciones de tratamiento de riesgo de seguridad de la información elegidas.
3. Formular el plan de tratamiento de riesgo de seguridad de información.
4. Obtener la aprobación del plan de tratamiento de riesgo de seguridad de información y aceptación de los riesgos residuales de seguridad de información por parte de la Dirección de la Unidad Administrativa correspondiente.
5. Realizar las acciones a implementar descritas en el PCN vigente del Instituto FONACOT.

XI. DETERMINACIÓN PARA LA GESTIÓN DE INCIDENTES.

El Instituto FONACOT gestiona los incidentes de acuerdo con la siguiente clasificación.

- Incidentes Cibernéticos.
- Incidentes de Seguridad de la Información.

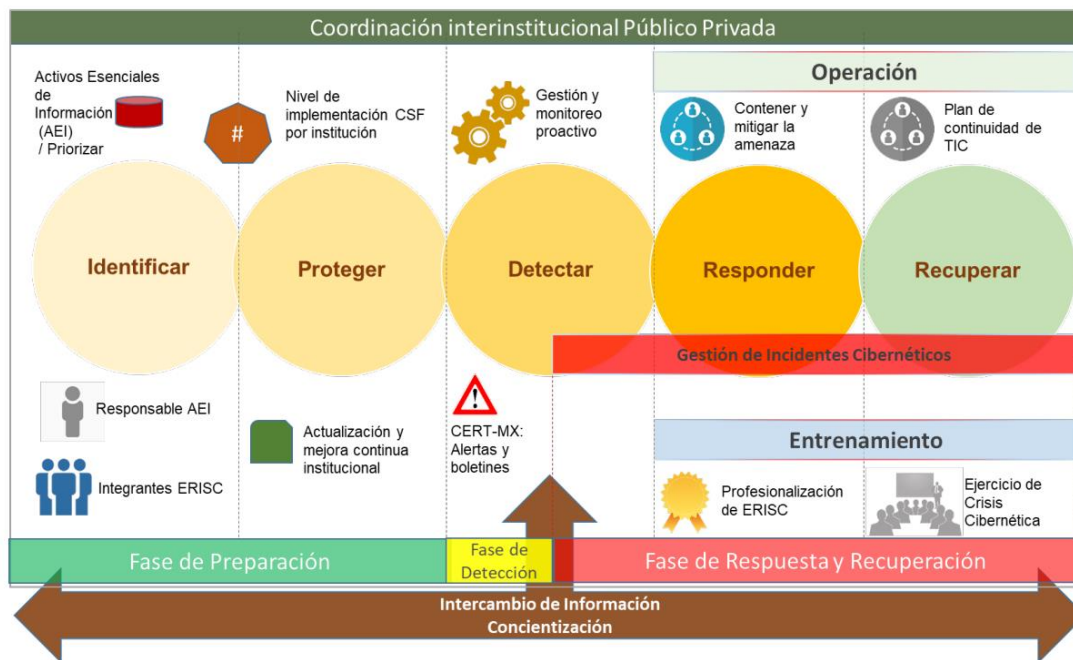
XI.I. Incidentes Cibernéticos.

Los incidentes cibernéticos se clasifican de la siguiente manera, esto, de acuerdo con el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

Criterios de determinación del nivel de criticidad de los incidentes cibernéticos		
Nivel	Clasificación	Tipo de incidente
CRÍTICO	Ataque multivector.	APT.
MUY ALTO	Código dañino.	Distribución de malware.
		Configuración de malware.
	Intrusión.	Sustracción de equipo de Centro de Datos.
	Disponibilidad.	Sabotaje en infraestructura de TIC.
ALTO		Interrupciones en servicios de TIC.
	Código dañino.	Sistema infectado.
	Código dañino / Intrusión.	Servidor C&C.
		Compromiso de aplicaciones.
	Intrusión / Intento de intrusión.	Compromiso de cuentas con privilegios.
		Ataque desconocido.
	Disponibilidad.	DoS.
	Disponibilidad / Compromiso de la información.	DDoS.
		Acceso no autorizado a la información.
	Compromiso de la información / fraude.	Modificación no autorizada de información.
	Pérdida de datos.	
	Phishing.	
	Contenido abusivo.	Discurso de odio.
MEDIO	Obtención de información.	Ingeniería social.
	Intento de intrusión.	Explotación de vulnerabilidades conocidas.

Criterios de determinación del nivel de criticidad de los incidentes cibernéticos		
Nivel	Clasificación	Tipo de incidente
ALTO	Intrusión / Intento de intrusión.	Intento de acceso con vulneración de credenciales.
		Compromiso de cuentas sin privilegios.
	Disponibilidad.	Mala configuración.
	Uso no autorizado de recursos de TIC.	Uso indebido de recursos de TIC.
	Fraude / Vulnerable.	Derechos de autor.
		Criptografía débil.
	Vulnerable / Contenido abusivo.	DDoS Amplificado.
		Servicios con acceso potencial no deseado.
		Revelación de información.
		Sistema vulnerable.
Spam.		
BAJO	Obtención de información.	Escaneo de redes (scanning).
	Obtención de información / Otros.	Análisis de paquetes (sniffing).
		Otros.

Para la atención de los incidentes cibernéticos, el Instituto FONACOT cuenta con la Política de Gestión de Incidentes alineada con el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. Su funcionamiento es el siguiente.



	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

XI.II. Seguridad de la Información.

Los incidentes relacionados a la seguridad de la información se clasifican de la siguiente manera:

Tipo de activo	Amenaza	Vulnerabilidad
Datos / Información	Modificación accidental de la información.	Modificación accidental de la información del Instituto FONACOT por medio de un error humano u omisión.
	Modificación intencional de la información.	Modificación intencional de la información del Instituto FONACOT, con ánimo de obtener un beneficio o causar un perjuicio.
	Fugas de información.	Revelación accidental de la información por personal laboral del Instituto FONACOT por indiscreción u omisión de la importancia de la información por medio verbal, medios electrónicos, soporte en papel o cualquier medio extraíble.
	Divulgación de información.	Divulgación intencional de la información del Instituto FONACOT, con ánimo de obtener un beneficio o causar un perjuicio por medio verbal, medios electrónicos, soporte en papel o cualquier medio extraíble.
	Destrucción de información.	Destrucción intencional de información del Instituto FONACOT, con ánimo de obtener un beneficio o causar un perjuicio.
	Pérdida de información.	Pérdida accidental de la información del Instituto FONACOT por error humano u omisión.
Criptografía	Modificación accidental de la llave criptográfica.	Modificación accidental de la llave criptográfica del Instituto FONACOT por medio de un error humano u omisión.
	Manipulación de la llave criptográfica.	Uso indebido de la llave criptográfica del Instituto FONACOT.
	Divulgación de la llave criptográfica.	Divulgación intencional de la llave criptográfica del Instituto FONACOT, con ánimo de obtener un beneficio o causar un perjuicio por medio verbal, medios electrónicos, soporte en papel o cualquier medio extraíble.
	Robo de llave criptográfica.	Sustracción de la llave criptográfica sin contar con la autorización pertinente.
Aplicaciones (Software)	Acceso no autorizado al sistema.	Se accede de manera mal intencionada al sistema aprovechando un fallo del sistema de identificación y autorización.
	Virus, Malware o código malicioso.	Propagación de software mal intencionado como: spyware, gusanos, troyanos, bombas lógicas, etc.
	Vulnerabilidades de los programas (injection, XSS, etc.).	Defectos en el código que dan pie a una operación defectuosa, con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
	Hackers / Crackers.	Persona que altera intencionalmente el funcionamiento de los programas, persiguiendo un beneficio directo.

Tipo de activo	Amenaza	Vulnerabilidad
	Denegación de servicio.	Carencia de recursos suficientes que provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	Destrucción de registros (logs).	Eliminación intencional o accidental de registros.
	Abuso de privilegios de acceso.	Cada cuenta tiene un nivel de privilegios para un determinado propósito; se abusa del nivel de privilegios cuando se realizan tareas que no son de su competencia incrementando el nivel de riesgo.
	Sistemas no actualizados.	Defectos en los procedimientos o controles de actualización que no permite actualizar sistemas.
	Modificación intencional de la información.	Modificación intencional de la información utilizando permisos de escritura.
	OWASP Top 10.	Vulnerabilidades del OWASP Top 10 sin remediar en las aplicaciones del Instituto FONACOT.
Aplicativo Móvil	Ejecución con privilegios innecesarios.	Dentro del código fuente de la aplicación, se puede ejecutar ciertos comandos.
	Exposición de datos sensibles.	La aplicación permite la captura de pantalla aun cuando se muestran datos sensibles.
		La aplicación mantiene la información sensible aun cuando se cambia entre aplicaciones.
		La aplicación mantiene cierto código de prueba aun cuando está haya sido ya lanzada en la tienda de aplicaciones.
	Un Factor de autenticación.	La aplicación no cuenta con un doble factor de autenticación, por lo cual se puede acceder con mayor facilidad.
	Tiempo de sesión indefinido.	La aplicación se mantiene activa aun cuando no ha sido utilizada por un tiempo.
	Información de llaves en el código.	La aplicación guarda las llaves públicas y/o privadas utilizadas en el cifrado de información, dentro del código fuente de la aplicación.
	Inexistentes mecanismos de bloqueo.	La aplicación no cuenta con un mecanismo de bloqueo de la cuenta, aun cuando se haya intentado ingresar a la misma después de un gran número de intentos.
	Equipos de root / emulación.	La aplicación no cuenta con un mecanismo de detección cuando esta sea ejecutada desde un dispositivo rooteado o desde un entorno de emulación, así como prevenir la ingeniería inversa sobre la aplicación.
	Uso de librerías con vulnerabilidades conocidas.	La aplicación utiliza librerías asociadas a cierto número de vulnerabilidades que no han sido remediadas.
Cifrado deficiente.	La aplicación utiliza un hash inseguro.	

Tipo de activo	Amenaza	Vulnerabilidad
	Denegación de servicio.	La aplicación no soporta grandes cantidades de solicitudes realizadas en el mismo periodo de tiempo.
Equipamiento Informático (Hardware)	Daños causados por fuego.	Incendio causado de manera natural o por la intervención humana.
	Daños causados por agua.	Inundaciones causadas de manera natural o por la intervención humana.
	Daños causados por sismos.	Sismos dentro de la CDMX, considerada como zona altamente sísmica.
	Desastres naturales.	Otros incidentes que se producen sin intervención humana como: rayos, tormentas eléctricas, contaminación, siniestro mayor, fenómeno climático, fenómeno volcánico, entre otras.
	Desastres industriales.	Fallos en los equipos de alimentación eléctrica ocasionando grave daño a la instalación.
	Interrupción de servicios o de suministros esenciales.	Interrupción de servicios o recursos de los que depende la operación de los equipos.
	Errores de mantenimiento / actualización de equipos.	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
	Caída del sistema por agotamiento de recursos.	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	Robo.	La sustracción no autorizada de equipo provoca directamente la carencia de un medio para prestar los servicios, es decir, una indisponibilidad.
Soportes de Información	Fugas de información.	Revelación de la información del Instituto FONACOT por parte del personal laboral utilizando cualquier medio extraíble.
	Indisponibilidad del sitio.	Indisponibilidad del sitio ocasionando que la información no este cuando sea requerida.
Equipamiento Auxiliar	Daños causados por fuego.	Incendio causado de manera natural o por la intervención humana.
	Daños causados por agua.	Inundaciones causadas de manera natural o por la intervención humana.
	Daños causados por sismos.	Sismos dentro de la CDMX, considerada como zona altamente sísmica.
	Desastres naturales.	Otros incidentes que se producen sin intervención humana como: rayos, tormentas eléctricas, contaminación, siniestro mayor, fenómeno climático, fenómeno volcánico, entre otras.
	Desastres industriales.	Fallos en los equipos de alimentación eléctrica ocasionando grave daño a la instalación.
	Errores de mantenimiento.	Deficiente o inexistente mantenimiento a los equipos.
Instalaciones Físicas	Daños causados por fuego.	Incendio causado de manera natural o por la intervención humana.

Tipo de activo	Amenaza	Vulnerabilidad
	Daños causados por agua.	Inundaciones causadas de manera natural o por la intervención humana.
	Daños causados por sismos.	Sismos dentro de la CDMX, considerada como zona altamente sísmica.
	Desastres naturales.	Otros incidentes que se producen sin intervención humana como: rayos, tormentas eléctricas, contaminación, siniestro mayor, fenómeno climático, fenómeno volcánico, entre otras.
	Desastres industriales.	Fallos en los equipos de alimentación eléctrica ocasionando grave daño a la instalación.
	Errores estructurales.	Ineficiente estructura del edificio.
	Terrorismo.	Actividad destructiva a la instalación con fin de dolo.
	Manifestaciones afuera del edificio.	Impedimento de acceso del personal laboral al edificio por obstrucción de entrada o de avenida.
	Huelgas de parte del sindicato.	Huelga del personal laboral del sindicato.
	Lugares remotos.	El personal laboral no cuenta con la infraestructura necesaria para continuar con la operación desde un lugar remoto.
Personal	Extorsión.	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
	Ingeniería social.	Utilización de técnicas como phishing para persuadir a una persona a realizar una acción solicitada con el fin de obtener contraseñas, o cualquier información relacionada con la persona o el Instituto FONACOT, usualmente esto se realiza por medio del correo electrónico.
	Indisponibilidad del personal laboral.	Ausencia del personal laboral de trabajo por motivos personales o médicos, así como también las huelgas o faltas no justificadas.
	Falta de capacitación para el personal laboral.	El personal laboral no cuenta con los conocimientos necesarios para continuar con la operación desde un lugar remoto.
	Violación de las políticas internas.	Violación o desconocimiento de las políticas internas del Instituto FONACOT.
	Mal manejo de la información confidencial.	La información confidencial se muestra visible a cualquier persona (contraseñas en "post-it").
	Conocimiento deficiente u obsoleto.	Falta de entrenamiento / capacitación al personal laboral para mantener actualizado el conocimiento sobre los procesos del Instituto FONACOT.
Contractual	Incumplimiento del contrato.	Incumplimiento en los acuerdos de nivel de servicio (SLA) o en los acuerdos de nivel de operación (OLA) que vienen establecidas dentro del contrato.
	Término del contrato.	Transferencia del conocimiento deficiente o inexistente al término del contrato.
	Incidente de seguridad dentro cualquier servicio arrendado.	Incidente ocurrido dentro de los servicios arrendados ocasionando fallas en el servicio del Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Tipo de activo	Amenaza	Vulnerabilidad
	Información almacenada dentro de los equipos arrendados.	Inexistente borrado seguro de la información dentro de los equipos al término de contrato.
	Indisponibilidad de personal de terceros.	Ausencia del personal de trabajo de terceros por motivos personales o médicos, así como también las huelgas o faltas no justificadas.
	Falta de cumplimiento en las políticas del Instituto FONACOT.	El proveedor no cumple con las Políticas de Seguridad del Instituto FONACOT.
	Falta de seguridad en las actividades del proveedor.	El proveedor no cumple con las mejores prácticas de seguridad de las cuales en manera enunciativa más no limitativa pueden ser: OWASP Top 10, MSTG, NIST, MITRE, SANS, entre otras.
Infraestructura Esencial	Ciberataques.	Conjunto de técnicas utilizadas por los atacantes para vulnerar la infraestructura esencial del Instituto FONACOT.

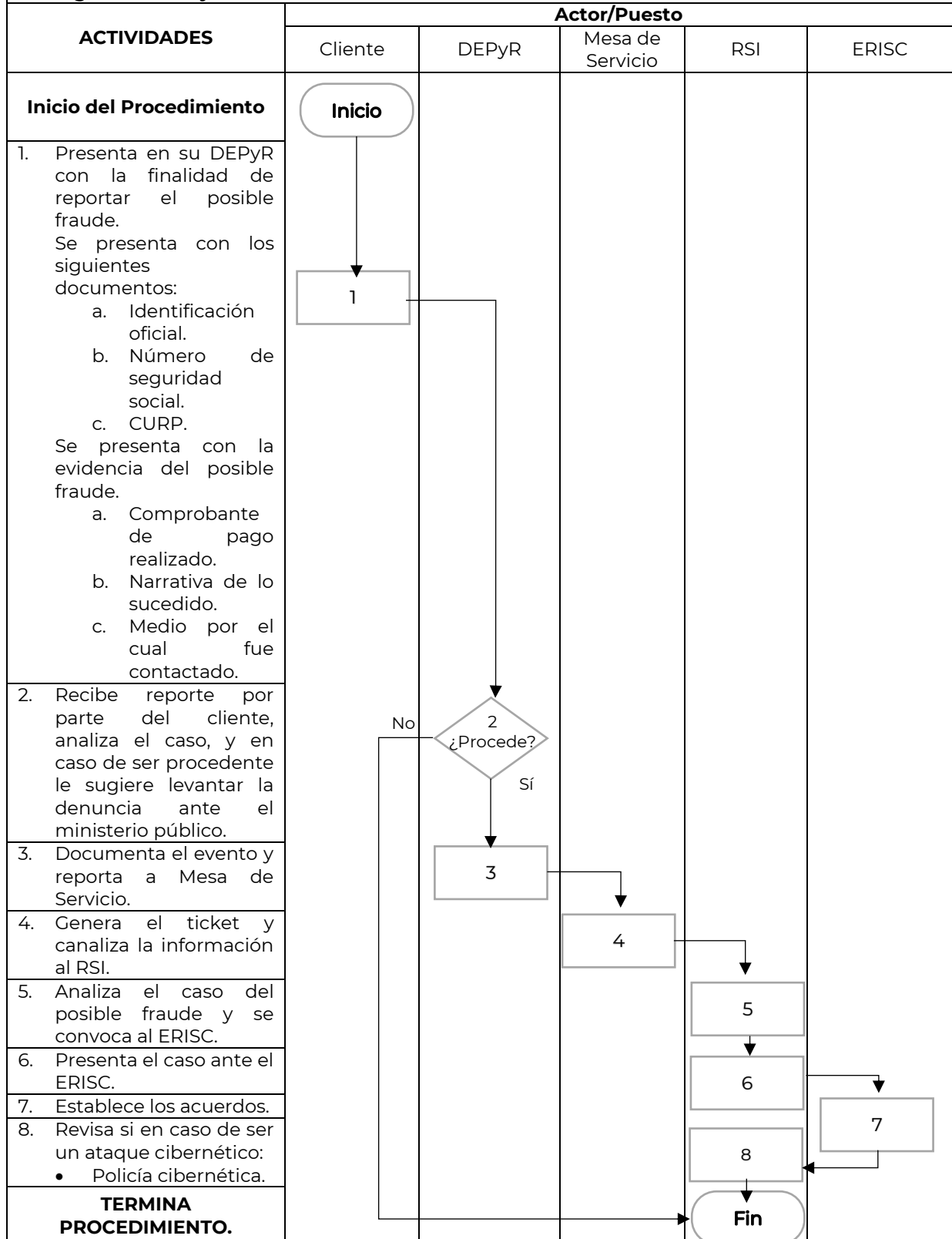
Para la atención de los incidentes de seguridad de la información, el Instituto FONACOT opera la Política de Gestión de Incidentes de Seguridad de la Información, y el Procedimiento de Gestión de Incidentes de Seguridad de la Información, los cuales están apegados a las buenas prácticas de la ISO 27001:2013 y de la NIST.SP.800-61r2.

XI.III. Eventos de Fraudes a Clientes del Instituto FONACOT.

El Instituto FONACOT atiende los eventos de fraude a clientes del Instituto FONACOT mediante el Protocolo de Atención al Fraude de Clientes del Instituto FONACOT, el cual se muestra a continuación.



Diagrama de Flujo del Protocolo de Atención al Fraude de Clientes del Instituto FONACOT.



XII. DETERMINACIÓN PARA LA GESTIÓN DE VULNERABILIDADES.

XII.I Plan Anual de Vulnerabilidades.

Se elabora el plan anual de vulnerabilidades sobre la infraestructura tecnológica, bases de datos, aplicativos web y móviles considerados críticos y debe presentar a las áreas involucradas del Instituto FONACOT para su ejecución y seguimiento.

XII.II Proceso de Identificación y Remediación de Vulnerabilidades.

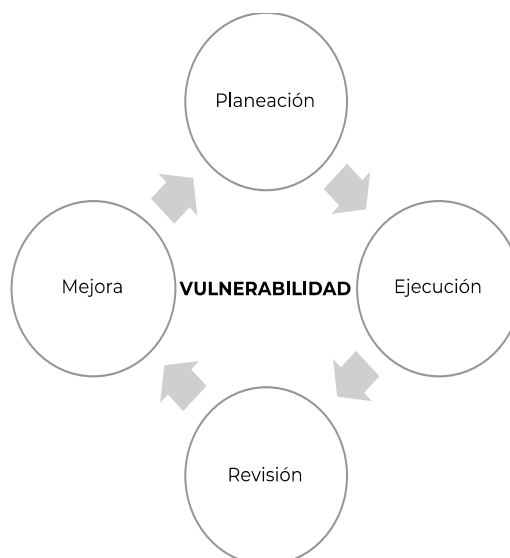
El Instituto FONACOT realiza las siguientes actividades:

- Seguridad - Realiza actividades de análisis de seguridad a la infraestructura tecnológica con la finalidad de identificar vulnerabilidades.
- Seguridad - Por cada una de la vulnerabilidad detectada se entrega al área involucrada del Instituto FONACOT en cuestión, el detalle, la criticidad y urgencia de corrección, incluyendo recomendaciones de corrección. Cada vulnerabilidad debe contar con un ID a través del cual se lleve a cabo el seguimiento a la atención y remediación del mismo, se debe documentar todo el seguimiento en la bitácora de seguimiento a vulnerabilidades.
- El área involucrada del Instituto FONACOT - Analiza la sugerencia de corrección y demás información recibida por el equipo de seguridad de la información.
- El área involucrada del Instituto FONACOT - Informa la decisión acerca de implementar la solución propuesta por el equipo de seguridad o bien considerar una solución alterna para la vulnerabilidad, justificando los motivos.
- El área involucrada del Instituto FONACOT - Implementa la solución y notifica al equipo de seguridad de la información los resultados.
- Seguridad - Confirma que la solución a la vulnerabilidad ha sido atendida.

XII.III Modelo para el Seguimiento a Vulnerabilidades.

Se da seguimiento a la remediación de las vulnerabilidades y que han sido reportadas a las áreas involucradas del Instituto FONACOT para su atención.

El seguimiento a las vulnerabilidades considera las siguientes fases:



 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Planeación – En esta fase el área involucrada del Instituto FONACOT presenta al equipo de seguridad de la información, la estrategia y la planeación para la atención de la incidencia.

El plan debe incluir la fecha de inicio y terminación de la remediación, persona líder y equipo responsable, ruta crítica, criterios de pruebas y aceptación, así como el presupuesto que llegara a ser necesario.

Ejecución – El área involucrada del Instituto FONACOT, lleva a cabo las actividades planificadas necesarias para llevar a cabo la mitigación de la vulnerabilidad.

Revisión – El área involucrada del Instituto FONACOT, debe realizar pruebas unitarias e integrales, así como de estrés y volumen, considerando todos los escenarios bajo los cuales fue detectada la vulnerabilidad.

El encargado de seguridad debe revisar estas pruebas proporcionadas por el área involucrada del Instituto FONACOT, solicitar al equipo de seguridad bajo su mando, la realización de la revisión de la mitigación de la vulnerabilidad y en caso de confirmar la corrección, otorgar su visto bueno.

Mejora – La mejora a la seguridad de la información se basa en ciclos de Deming (Planear (P), Hacer (H), Verificar (V), y Actuar (A)).

Adicionalmente, el equipo de seguridad realiza un control sobre el seguimiento de las vulnerabilidades con la finalidad de analizar la recurrencia por tipo de vulnerabilidad y el tiempo de atención con relación a la criticidad de la vulnerabilidad.

XIII. SEGURIDAD DE LA INFORMACIÓN EN LA TRANSICIÓN DEL IPV4 A IPV6.

El Instituto FONACOT propone los elementos de seguridad sobre las técnicas de transición a implementar que dicta la “Guía para la Transición al Protocolo de Internet versión 6 (Ipv6) en la Administración Pública Federal que emite la CEDN”, así como aquellas recomendaciones indicadas por el Comité de Supervisión para Ipv6.

El Instituto FONACOT identifica y realiza acciones para mitigar los riesgos potenciales a la seguridad de la información que se encuentren asociados a la transición.

El Instituto FONACOT verifica que los bienes y servicios de TIC actuales y futuros sean capaces de operar en ambientes Ipv6 nativos, así como, el cumplimiento de los estándares técnicos emitidos por la CEDN.

XIV. DETERMINACIÓN DE LA EVALUACIÓN Y MEJORA CONTINUA DE LOS ESTÁNDARES TÉCNICOS.

El Instituto FONACOT verifica que los estándares técnicos, así como las mejores prácticas aplicables de seguridad de la información, sean consideradas en los procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios.

El Instituto FONACOT evalúa técnicamente el desempeño de los controles de seguridad de la información implementados y realiza la mejora continua, a través de auditorías que pueden ser ejecutadas por:

- Un tercero, especializado en revisiones de seguridad.
- Dirección de Auditoría Interna.
- Subdirección General de Contraloría, Planeación y Evaluación.
- Autoridades regulatorias o supervisoras del Instituto FONACOT.

XV. MEJORA CONTINUA.

El Instituto FONACOT basa su MGSI a través de la Mejora Continua en un Ciclo Deming (PHVA).

XVI. DETERMINACIÓN DE POLÍTICAS, PROCEDIMIENTOS, METODOLOGÍAS Y ANEXOS DE SEGURIDAD DE LA INFORMACIÓN.

El Instituto FONACOT cuenta con políticas, procedimientos, protocolos, metodologías y anexos de seguridad de la información.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

1. POLÍTICA DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

Esta política proporciona una serie integrada de medidas de protección que deben aplicarse en el Instituto FONACOT, de esta manera se asegura la disponibilidad, integridad y confidencialidad de todas sus redes, aplicaciones e información.

A pesar de que esta política se enfoca en la clasificación de recursos y protección informática, se deben tomar en cuenta los requerimientos de las políticas de Seguridad de la Información existentes al momento de diseñar las medidas preventivas.

2. RESPONSABILIDAD SOBRE LOS ACTIVOS.

El Instituto FONACOT debe identificar todos los activos dentro del alcance del MGSI como son las redes, aplicaciones, equipos físicos o información y definir las responsabilidades de protección a cada uno de ellos. La DIT es la responsable de gestionar y mantener actualizado el inventario de activos tecnológicos.

2.1. Inventario de Activos.

El Instituto FONACOT debe mantener actualizado el inventario de activos.

El inventario de activos debe cumplir con lo estipulado en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y su Anexo Identificación de Activos Esenciales de Información de los Múltiples Involucrados, dicho inventario debe tener al menos la siguiente información.

- a) Site – KIO.
- b) Origen.
- c) Unidad de procesamiento.
- d) Estatus.
- e) Hostname.
- f) Aplicación.
- g) Nube.
- h) Descripción.
- i) Plataforma.
- j) Ubicación física.
- k) Máscara de subred.
- l) Gateway.
- m) VLAN ID.
- n) Ambiente.
- o) IP Producción.
- p) IP backup / mgt.
- q) IP Pública.
- r) Marca / Modelo.
- s) Número de serie.
- t) Hardware físico / virtual.
- u) Sistema Operativo.

El RSI requiere contar con el inventario de activos actualizado de manera periódica.

2.2. Propiedad de los Activos de Información.

Los activos físicos (ej. hardware), activos lógicos (ej. software almacenado en una computadora) y activos de Información, deben contar con una persona que sea custodio del activo asignado.

Las personas que son custodios de los activos de información (ej. un sistema de información y sus datos asociados) deben ser personal laboral de base del Instituto FONACOT, no asesores, personal laboral temporal, proveedores de servicios ni cualquier otro recurso externo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.2.1. Asignación de la Propiedad.

La propiedad de los principales activos de información debe ser asignada antes de que dichos activos sean utilizados en un ambiente de producción. La propiedad de los activos secundarios (ej. un archivo de algún documento) debe ser responsabilidad inicial de la persona que custodia el activo o de la persona para quien el activo secundario fue creado.

El personal que sea custodio de los activos deben:

- Asegura que la información y los activos sean clasificados apropiadamente.
- Define y revisa periódicamente el acceso a los activos.
- Asegura el manejo adecuado del activo cuando esté sea destruido o eliminado.

2.2.2. Reasignación de la Propiedad.

Si la persona que tiene la custodia actualmente no puede continuar con esa función, la administración local debe reasignar la propiedad a otra persona de acuerdo con el perfil.

La SIT debe actualizar el inventario de los activos de Información para reflejar los cambios en la propiedad de los activos de Información.

2.2.3. Responsabilidades para Custodiar los Activos de Información.

Las personas que custodian los activos deben poner los activos bajo custodia y delegar la responsabilidad para apoyar las operaciones y mantener las actividades asociadas con el activo. Esto se realiza en funciones esenciales, incluyendo la protección apropiada al activo.

Las personas que custodian los activos también deben ser responsables de realizar las funciones delegadas. Poner un activo bajo custodia de otra persona o entidad no exime de ninguna manera a las personas custodios de los activos de la responsabilidad de proteger correctamente el mismo.

2.3. Uso Aceptable de Activos.

Las personas que custodian los activos deben responsabilizarse del uso adecuado a los activos a su cargo; esto de acuerdo con el cumplimiento de las siguientes políticas de Seguridad de la Información del Instituto FONACOT:

- Política de pantalla y escritorio limpio.
- Política de control de acceso.
- Política de Relación con Terceros.

2.4. Devolución de los Activos.

Las personas que custodian los activos en el Instituto FONACOT deben devolverlos a la terminación del empleo, contrato o acuerdo.

2.5. Manejo de Activos.

El manejo de activos se debe apegar a las políticas de seguridad y procedimientos del Instituto FONACOT correspondientes:

- Política de control de acceso.
- Política de Criptografía.
- Política de pantalla y escritorio limpio.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3. GESTIÓN DE LOS SOPORTES.

3.1. Gestión de Medios Removibles.

El Instituto FONACOT debe tener un listado de los medios removibles que se utilizan en cada área. El listado debe contener la siguiente información:

- Tipo de medio removible (Memorias USB, disco flexible, etc.).
- Clasificación de la información que se está almacenando en el medio removible.
- Destinatario de la Información.
- Persona que sea custodio del medio removible.

El uso de medios de comunicación removibles debe ser controlado y protegido con base en su clasificación de la información almacenada en los medios.

Las personas que custodian la información deben asegurar que todos los medios de almacenamiento removibles son almacenados en un ambiente seguro.

La información contenida en medios de almacenamiento de proveedores debe eliminarse antes de que estos sean devueltos.

Por último, el Instituto FONACOT se asegura del cumplimiento al procedimiento para habilitar/deshabilitar el uso de medios de almacenamiento externos en equipos de cómputo.

3.2. Eliminación de Soportes.

El Instituto FONACOT se asegura del cumplimiento al procedimiento de borrado seguro en los medios removibles propiedad del Instituto FONACOT (Memorias USB, disco flexible, etc.) dicho procedimiento debe contar con al menos las siguientes características:

- Registrar la eliminación de los elementos sensibles siempre que sea posible con el fin de mantener una evidencia de auditoría.
- Realizar la eliminación de activos físicos y/o digitales con al menos un método de destrucción de la información, como son: magnetización, destrucción física (desintegración, pulverización, fusión, incineración, trituración), sobre escritura mínima de 3 pasadas.
- Realizar un backup de la información almacenada en el medio removible, si es que así lo requiera, antes de su destrucción.

3.3. Soportes Físicos en Tránsito.

El Instituto FONACOT debe proteger los medios que contengan información contra acceso no autorizado, mal uso o modificación de la información durante su transportación.

Para el transporte de los medios removibles, el Instituto FONACOT debe tomar en cuenta las distintas consideraciones:

- Se utilizan únicamente los servicios de mensajería que estén autorizados por el Instituto FONACOT.
- Todos los soportes que tengan información clasificada como confidencial, deben estar cifrado y la clave para descifrarlo tendrá que ser enviado a través de otro medio distinto.
- Adoptar controles adicionales cuando se crea necesario a fin de proteger la integridad de la información, estos controles pueden ser:
 - Uso de sobres sellados.
 - Acuse de recibido.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2. POLÍTICA DE CONTROL DE ACCESOS.

1. INTRODUCCIÓN.

Esta política tiene el objetivo de proporcionar los requerimientos mínimos para la definición y operación de los controles de acceso y administración de privilegios de las cuentas que tienen acceso a la información del Instituto FONACOT.

Los principales elementos de protección que exige esta política son:

- Los requerimientos para tener acceso físico a instalaciones del Instituto FONACOT de personal laboral y terceros.
- Los requerimientos para tener acceso lógico a cualquier recurso informático del Instituto FONACOT por medio de autenticación.
- Los requerimientos mínimos para la autenticación de la identidad del personal basados en la clasificación de la información para la cual el personal autorizado requiere tener acceso.
- Control de acceso a activos lógicos basado en listas de control de acceso.
- Funciones y responsabilidades referentes al control de acceso, autenticación y acceso a operaciones privilegiadas.

Esta política aplica a todo el personal interno, terceros, cuentas privilegiadas y no privilegiadas.

2. CONTROL DE ACCESOS.

2.1. Controles Físicos de Entrada.

- Los edificios del Instituto FONACOT deben contar con muros de concreto y estar cerrados, de tal manera que las entradas resguardadas por personal laboral de seguridad sean la única manera de acceder físicamente al Instituto FONACOT.
- Las puertas de acceso deben contar con refuerzo físico como son cortinas de metal después del cierre de trabajo en Áreas Seguras.
- Las áreas aseguradas deben estar protegidas con controles de entrada apropiados, estos pueden incluir vigilancia, acceso con dispositivos biométricos, acceso con llave.
- Se tiene una zona de recepción vigilada por personal, u otros medios para controlar el acceso físico a las instalaciones.
- El personal laboral del Instituto FONACOT debe portar de manera visible su gafete de autenticación, es personal e intransferible, por lo cual ninguna persona no autorizada podrá acceder a las instalaciones utilizando el mismo acceso de una persona autorizada. El personal laboral que haya olvidado su gafete de identificación debe obtener un gafete temporal en la recepción, dejando a cambio una identificación oficial con fotografía. Los gafetes de identificación que se encuentren extraviados o se sospeche de su robo, deben ser reportados al encargado del control de acceso que esté en turno.
- El acceso para las personas que terminan la relación laboral o contractual dentro del Instituto FONACOT, deben eliminarse inmediatamente de listas y/o sistemas de control de acceso físico, a fin de que no se les otorgue el ingreso a las instalaciones del Instituto FONACOT.
- Se realiza monitoreo dentro de las instalaciones del Instituto FONACOT.
- Con el objeto de proteger los activos, de accesos no autorizados, la recepción funge también como área de canalización a las áreas para la entrega de material, equipos y documentación general.
- Para el ingreso por la rampa del edificio sede, al área de carga y descarga de los materiales y alimentos; todo personal laboral debe enviar notificación vía correo o escrito a la Dirección de Recursos Materiales y Servicios Generales para su ingreso.
- Los paquetes, cajas y maletas que ingresen o salgan de las instalaciones son inspeccionados para evitar amenazas potenciales, así como salidas no permitidas de equipos de cómputo.
- El personal laboral, está obligado a cuestionar la estancia de cualquier persona que no conozcan y que se encuentre en las instalaciones sin alguna escolta interna. Si los visitantes no pueden justificar y/o

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

mostrar una identificación válida, ellos deben ser escoltados a la recepción del edificio, para que se retiren.

- Todas las oficinas se deben mantener cerradas cuando no se encuentre personal laboral dentro de ellas.

2.2. Acceso a la Información del Instituto FONACOT.

- El acceso a la información digital del Instituto FONACOT debe estar controlada por la autenticación del equipo de cómputo y un segundo factor de autenticación hacia los sistemas y aplicaciones que sean necesarias para la realización de las funciones del personal laboral del Instituto FONACOT.
- La asignación del acceso a la información digital del Instituto FONACOT debe estar basada en los roles y responsabilidades del Instituto FONACOT, así como la segregación de funciones de ser necesario para la seguridad de la información. Si se requiere un acceso adicional a los proporcionados, por estos principios se debe realizar la petición de acceso, sincronización y/o administración de información según se necesite, esta solicitud debe estar justificada por las actividades a realizar y aprobada por un rango superior al solicitante.
- Las entradas asociadas con un archivo, directorio o elemento de una base de datos correlativa deben contener, al menos, el ID de la cuenta, el ID del grupo o algún otro identificador, así como el derecho al acceso.
- El área de sistemas debe controlar el acceso único de cada persona, evitando sesiones simultáneas.
- Se debe gestionar el acceso a entornos distribuidos e interconectados, como lo son el inicio de sesión unificado (Single Sign On). El acceso de lectura o escritura a la información (electrónica) con un nivel de confidencialidad, debe estar controlado con base en los derechos de acceso.
- Se debe restringir el acceso con base en los siguientes derechos de acceso:
 - De creación.
 - De lectura.
 - De escritura.
 - De ejecución.
- El personal que custodia los activos debe otorgar el acceso a los activos de información únicamente por el período específico según la necesidad documentada del negocio.
- Los permisos concedidos son asignados de manera personal e intransferible.
- El personal que custodia los activos puede elegir la fecha de vencimiento del acceso a cualquier recurso. El acceso otorgado al personal temporal también debe tener una fecha de vencimiento.
- Los custodios y las personas que hacen uso de los activos deben verificar continuamente la necesidad de contar con todos los derechos de acceso otorgados.
- Se deben realizar revisiones de los derechos de acceso asociados con las cuentas tanto del personal como de terceros, por lo menos cada trimestre. Se debe generar registro de estas revisiones.
- Se deben realizar revisiones de accesos asociados a los perfiles de terceros o personal del Instituto FONACOT con el objetivo de validar si el perfil existe en el directorio activo.
- Se debe realizar una revisión anual de los derechos de acceso a la información tanto de personal laboral como de terceros. Durante la revisión, el administrador de seguridad debe proporcionarle al personal que custodia los activos un resumen de los derechos de acceso a sistemas y aplicaciones.
- Se debe generar registro de la revisión anual de los derechos de acceso.
- De existir cambios en las funciones asignadas, se requiere la notificación al área de sistemas para realizar la modificación en las aplicaciones, sistemas o equipos definidos con los derechos de acceso correspondientes a las nuevas funciones y/o eliminar los requerimientos para el acceso existente.
- La Dirección de Recursos Humanos o responsable del área debe informar a través de correo electrónico al personal encargado de la administración de la seguridad sobre los cambios en el estatus de empleo o responsabilidades.
- Los controles de acceso para el personal laboral que terminó su relación con el Instituto FONACOT deben eliminarse inmediatamente, así como los proveedores que dejan de prestar sus bienes o servicios para el Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.3. Acceso a las Redes y los Servicios de la Red.

Los sistemas de red regulan la capacidad de conectar la mayoría de los servicios de información sin requerir la presencia física del personal. Las conexiones inseguras a los servicios de red pueden afectar todo el Instituto FONACOT por lo que este control es particularmente importante para las conexiones de red con un nivel de confidencialidad, aplicaciones importantes o personal laborando en lugares externos.

- El personal responsable del sistema o aplicación debe realizar un inventario de control de acceso que tendrá la finalidad de informar altas, cambios y cancelaciones de accesos.
- Los dispositivos y sistemas de red del Instituto FONACOT deben configurarse adecuadamente y sujetarse a controles de acceso para prevenir modificaciones y accesos no autorizados a los activos de información.
- El registro de las personas que harán uso de estos servicios se llevará a cabo por medio de una solicitud de acceso.
- Revisar los accesos a la red cada 6 meses, después de cambios mayores o cuando se produzca un incidente de seguridad.
- Retirar los accesos a la red de los equipos necesarios, cuando se considere que la seguridad de la información está comprometida.
- Debe controlarse y segregarse adecuadamente el riesgo latente del anonimato en la red para prevenir mal uso o accesos no autorizados. Se debe proporcionar acceso directo y exclusivo a los servicios que la personal tiene autorizado.

2.4. Autenticación para Conexiones Entrantes.

Antes de establecer una sesión de conexión en la red del Instituto FONACOT, el personal y los terceros autorizados deben ser identificados y autenticados.

2.5. Autenticación para Conexiones Salientes.

Para las conexiones desde el interior de la red del Instituto FONACOT hacia un nodo de red externo que puedan exponer al Instituto FONACOT a riesgos de negocio significativos (por ejemplo: transacciones de negocio electrónicas), el destino de red externa con el cual se llevan a cabo transacciones debe identificarse y autenticarse.

Si una aplicación transfiere información por la red, debe estar protegida de acuerdo con la clasificación proporcionada a la información.

2.6. Protección de Acceso Remoto a través de Puertos de Comunicación.

- La solicitud para el acceso a puertos de comunicación para conexiones remotas debe ser presentada por la Dirección solicitante ante el RSI, dicha solicitud debe contener la justificación detallada.
- El RSI posterior a su valoración, niega o aprueba la solicitud.
- Los accesos a puertos de comunicación como 22, 3389, 1521, 1433, 7001, 7005, 8001, 9001 y VNC – 5902 se deben llevar a cabo conforme al PROCEDIMIENTO DE POLÍTICAS DE COMUNICACIÓN.

2.7. Segregación de Redes.

- Los segmentos de la red del Instituto FONACOT deben separarse lógicamente para garantizar la separación de funciones incompatibles y los privilegios de acceso.
- Los requerimientos de acceso y la evaluación de riesgos, la red del Instituto FONACOT debe dividirse en dominios o segmentos apropiados. Estos incluyen al menos los siguientes:
 - Desarrollo.
 - Operaciones.
 - Red perimetral.
 - Red invitados.
 - Red LAN.
 - Red DMZ.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.8. Control de Conexión de Red.

- Las capacidades de acceso de cada cuenta a la red, deben limitarse sólo a las definidas y aprobadas.
- Los servicios para los cuales el nivel de acceso está determinado por la propia naturaleza de conexión de red, deben ser identificados, documentados y se debe controlar su acceso. Estos servicios deben incluir, pero no limitarse, a los siguientes:
 - Aplicaciones de red, como el correo electrónico.
 - Herramientas de transferencia de archivos.
 - Acceso interactivo (por ejemplo: línea de comandos).

2.9. Control de Ruteo de Red.

El ruteo de red, desde el punto de acceso remoto hasta el punto destino en la intranet, debe garantizar que el tráfico se mantiene dentro de los segmentos y nodos de red para los cuales ha sido autorizado. Los controles para lograr esto, incluyen, pero no se limitan a los siguientes:

- Deshabilitar el Roaming de red ilimitado.
- Definición de dominios lógicos para aislar segmentos de la red y la implantación de Gateways de seguridad (por ejemplo: firewalls) para controlar el tráfico entre dominios lógicos.
- Predefinición de la ruta de red para prevenir cualquier intervención y eliminar la oportunidad de explorar la red.

2.10. Seguridad de Servicios de Red.

- El personal que sea custodio de los sistemas o dispositivos de red debe informarse de las ventajas y limitantes de seguridad de dichos sistemas o dispositivos. Deben implantarse medidas apropiadas para administrar el riesgo de las limitaciones de seguridad que se tienen en los activos de información.
- Las características y limitantes de los activos de información deben ser revisadas, documentadas y aprobadas antes de que estos sean liberados al ambiente de producción.
- Los activos de información se deben mantener actualizados con sus respectivos parches y actualizaciones de seguridad.

2.11. Acceso y Privilegios

Para mantener el registro y administración de las cuentas y sus privilegios en el Instituto FONACOT, se debe realizar por medio de la generación de tickets que permita garantizar que la documentación y la autorización correspondientes se lleven a cabo, esto aplica para alta y baja de cuentas, así como el mantenimiento de los privilegios otorgados, los cuales pueden ser modificados para cada persona de acuerdo con los movimientos en su puesto de trabajo o actividades asignadas.

2.12. Identificación del Personal.

- Cada persona debe tener un identificador único asignado.
- No se permite la existencia de identificadores genéricos.

2.13. Requerimientos del Negocio para Control de Acceso.

Los privilegios de acceso son otorgados con base al mínimo privilegio, es decir, sólo deben otorgarse los privilegios requeridos por el rol o puesto de la persona para desempeñar sus funciones.

3. PRIVILEGIOS DE ACCESO.

- Los privilegios de accesos de manera enunciativa más no limitativa se refieren a: cuentas privilegiadas y no privilegiadas (sistema, creación, lectura, actualización, escritura, de eliminación, etc.).

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- El RSI es responsable de la autorización de privilegios de acceso para los recursos de información respectivos. Adicionalmente, se debe tener la documentación sobre quienes tienen acceso a cuáles recursos, dicha documentación debe mantenerse resguardada. La parte que autoriza debe verificar que el tipo de acceso solicitado sea apropiado para el rol o puesto y las responsabilidades inherentes.
- Debe proveerse al personal una descripción escrita de sus privilegios de acceso, asimismo, debe verificarse su entendimiento y que están de acuerdo con las condiciones de acceso establecidas.
- Los terceros deben ser sujetos al cumplimiento de todas las políticas del Instituto FONACOT cuando accedan o utilicen activos. No debe otorgarse ningún privilegio de acceso hasta que se hayan completado los procedimientos de autorización respectivos.
- Para la solicitud de cuentas se debe seguir el procedimiento de gestión de cuentas del Instituto FONACOT.

3.1. Mantenimiento de Privilegios de Acceso.

El personal custodio de los activos de información debe realizar revisiones periódicas sobre los privilegios de acceso con el objetivo de identificar e inhabilitar cuentas genéricas y en desuso. Estas revisiones deben realizarse al menos cada seis meses, considerando las cuentas de personal laboral del Instituto FONACOT, así como, los terceros relacionados con bienes o servicios.

3.2. Administración de Privilegios de Acceso.

- Apegarse al Procedimiento de Gestión de Cuentas.
- Las cuentas o accesos con altos privilegios en los sistemas operativos, aplicativos, herramientas, redes, bases de datos, están restringidos, dichos accesos deben ser gestionados por el administrador del contrato y concederse a través de una solicitud formal que incluya la justificación detallada y fundamentada, la aprobación debe ser provista por el RSI. Los accesos privilegiados deben ser limitados, específicos, justificados plenamente y antes de ser evaluada la autorización, se deben agotar las posibilidades de poder realizar el acceso con identificadores y privilegios estándares.
- Se deben generar bitácoras respecto al uso de las cuentas privilegiadas y/o cuentas mancomunadas, que incluya al menos lo siguiente:
 - Motivo o justificación del acceso.
 - Nombre de la persona que será custodio de la cuenta.
 - Fecha y hora en la que se utilizó la cuenta.
- Estas bitácoras son implementadas en la infraestructura crítica del Instituto FONACOT.
- Las cuentas privilegiadas y mancomunadas deben ser gestionadas a través de una herramienta PAM.
- El acceso privilegiado debe revisarse periódicamente con la finalidad de identificar y remover cuentas de las personas que ya no laboran en el Instituto FONACOT, cambios de puesto, funciones de trabajo y cuentas en desuso por más de 90 días. Esta revisión debe ejecutarse al menos, trimestralmente.

3.3. Revocación de Privilegios de Acceso.

- En los casos de cambios de puesto o funciones dentro del Instituto FONACOT (por ejemplo: transferencia, promoción, finalización de relación contractual), la Subdirección de Área y la persona que es el custodio del activo de información o proceso de negocio deben ser notificados de manera inmediata por quien lo solicita. Los privilegios de acceso deben ser revocados o reasignados (si es apropiado) inmediatamente después de la notificación.
- En el caso del personal laboral o proveedores temporales, si se conoce la fecha de finalización de relación contractual, los privilegios de acceso respectivos deben tener una fecha automática de terminación, en lo posible, conforme a las fechas de contrato negociadas.

3.4. Notificación de Bajas o Cambios en los Recursos Humanos.

En caso de finalización de relaciones contractuales, la DRH debe realizar las notificaciones y acciones apropiadas de manera inmediata o por adelantado, para asegurar que tanto el acceso lógico como físico se ha cerrado y

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

que todos los activos del Instituto FONACOT sean devueltos antes de que el personal laboral involucrado abandone las instalaciones. Esto incluye, como mínimo, notificar a las áreas de SGTIC y DRMySG, así como al RSI.

En caso de que terceros tengan cuentas con privilegios, la persona que administra el contrato del servicio del tercero o la SGTIC deben notificar de manera inmediata la baja o actualización de las cuentas con privilegios que tengan acceso a los recursos de TIC del Instituto FONACOT.

- La SGTIC debe tener una cuenta con privilegios de administrador en todos los aplicativos y bases de datos con la finalidad de poder deshabilitar cuentas cuando el contrato de los proveedores haya terminado.
- El RSI debe solicitar periódicamente el reporte de baja de las cuentas asignadas al personal de terceros y tomar las acciones que correspondan.

4. CONTRASEÑAS.

- a. Debe forzarse el uso de contraseñas individuales por medio de las aplicaciones y sistemas operativos, con el objetivo de mantener el registro de acceso y poder asignar responsabilidades respecto a su uso.
- b. Para los sistemas protegidos por contraseñas, el personal debe tener la capacidad de cambiar sus contraseñas, de modo que se restrinja el conocimiento de estas.
- c. Debe emplearse la confirmación de cambio de contraseña, para prevenir errores futuros que nieguen el acceso legítimo.
- d. Las reglas aplicables a la creación y uso de contraseñas robustas deben documentarse y hacerse cumplir.
- e. Debe mantenerse un registro de contraseñas previamente utilizadas en los sistemas de administración de contraseñas para prevenir su reutilización.
- f. Las contraseñas no deben desplegarse en la pantalla cuando sean ingresadas a los sistemas.
- g. Los archivos de contraseñas deben almacenarse de forma cifrada dentro de la aplicación de manera separada de los datos para prevenir cualquier acceso no autorizado.
- h. Las contraseñas por omisión no deben utilizarse en los sistemas después de su instalación (aplicación o sistema operativo).
- i. Las contraseñas proporcionadas por fabricantes o distribuidores de software deben ser modificadas.
- j. Las contraseñas iniciales deben determinarse por el sistema de manera automática o por la persona que administre las contraseñas y estas contraseñas deben ser comunicadas al personal solicitante a través de un medio de comunicación seguro.
- k. Los identificadores de las cuentas y contraseñas son considerados información confidencial y deben administrarse de manera segura para prevenir su divulgación durante la configuración inicial de la cuenta.
- l. Las contraseñas iniciales o temporales deben modificarse inmediatamente después del primer acceso (el primer uso), este proceso debe ejecutarse en forma automática por el sistema.

5. RESPONSABILIDAD DE LOS RECURSOS HUMANOS.

El personal laboral y terceros deben ser conscientes acerca de sus responsabilidades respecto con los controles de acceso, en particular al uso de contraseñas y seguridad del equipo de cómputo que tienen asignado.

- a. Prevenir el acceso no autorizado y prevenir el mal uso de la información.
- b. Las cuentas deben ser utilizadas sólo por la persona quien tiene su custodia, por lo tanto, queda estrictamente prohibido el uso compartido de cuentas a excepción de las cuentas mancomunadas, mismas que deben ser gestionadas a través de una herramienta PAM.
- c. La contraseña debe contener un periodo de vencimiento, este periodo se definirá de acuerdo con las necesidades de la cuenta, sin exceder un periodo de un mes.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

5.1. Uso de Contraseñas.

El personal debe seguir las mejores prácticas en la selección y uso de sus contraseñas, considerando lo siguiente:

- Mantener la confidencialidad de sus contraseñas.
- Evitar contar con un registro de estas.
- Cambiar las contraseñas siempre que exista un indicio de que han sido comprometidas.
- Seleccionar contraseñas robustas.
- Cambiar sus contraseñas periódicamente.

Las contraseñas no deben ser reveladas ni compartidas, salvo en casos de emergencia, en los cuales se cuenta con la autorización de la Dirección de la Unidad Administrativa correspondiente. Una vez resuelta la situación de emergencia, el responsable directo de la cuenta debe cambiar la contraseña de inmediato.

5.2. Equipo de Cómputo Desatendido.

El personal debe garantizar que su equipo se encuentra seguro cuando queda desatendido por medio de bloqueo o finalización de sesión de trabajo, protección de pantalla a través de un protector de pantalla con contraseña.

5.3. Pantallas y Terminales Seguras.

- Los equipos de cómputo y terminales no deben dejarse desatendidos y deben protegerse a través del bloqueo de sesiones o apagado del equipo cuando este no se utilice.
- La información confidencial o de uso interno en papel o contenida en los medios de almacenamiento removible, debe resguardarse en un lugar seguro o al menos debe mantenerse fuera del alcance de personal laboral no autorizado cuando no se esté utilizando.
- Las máquinas de fax y fotocopiadoras deben ubicarse en lugares estratégicos a fin de evitar accesos no autorizados, debe verificarse diariamente que estos equipos no contengan información confidencial o de uso interno.
- Es responsabilidad de quien realiza actividades de impresión, envío o recepción de faxes y de fotocopiado asegurarse que las copias e impresiones no se queden en las máquinas de fax o fotocopiadoras.
- Para el uso de fotocopiadoras, el personal debe utilizar un código de acceso, evitando el uso no autorizado.

6. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES.

- Los sistemas operativos que soportan todos los activos de información del Instituto FONACOT deben configurarse apropiadamente y sujetarse a controles de acceso para prevenir modificaciones o accesos no autorizados.
- El acceso a las funciones provistas por el sistema operativo debe segregarse apropiadamente y asignarse con base en la necesidad requerida y debe sujetarse a controles apropiados para prevenir uso no autorizado.
- Los procedimientos de conexión deben adaptarse de manera que solo se disponga de la cantidad mínima de información para que el personal pueda autenticarse apropiadamente. Deben implantarse los siguientes controles en la medida de lo posible:
 - Los identificadores de sistema o aplicación no deben desplegarse hasta que el proceso de conexión se ha completado de manera exitosa.
 - La información de conexión debe validarse hasta que se completen correctamente todos los datos de entrada y no se haya identificado información de autenticación incorrecta que pueda ingresarse para intentar acceder fallidamente al sistema.
 - El número de intentos de acceso fallido al sistema debe limitarse a 3 intentos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- El tiempo establecido entre intentos de acceso fallido al sistema debe limitarse para prevenir ataques de fuerza bruta.
- La identificación y autenticación debe llevarse a cabo antes de tener acceso a los sistemas y aplicaciones.
- El acceso a los recursos de cómputo debe otorgarse conforme a roles y responsabilidades.
- El personal autorizado debe identificarse de manera única y ser verificados por el sistema antes de permitir el acceso a la red y recursos informáticos del Instituto.
- Al personal laboral y los terceros que justifiquen la necesidad de contar con acceso a los recursos informáticos del Instituto FONACOT, se les debe asignar un identificador único, esto con la finalidad de monitorear los accesos y las actividades realizadas.
- Se debe considerar la asignación de cuentas adicionales para acceder a recursos informáticos críticos, lo anterior tiene el objetivo de prevenir posibles problemas de inaccesibilidad en caso de contingencia.

6.1. Uso de Utilerías del Sistema.

- Debe restringirse a todo el personal el acceso a las utilerías del sistema que tienen la capacidad de sobrescribir controles del sistema o aplicación, excepto para aquellos que cuenten con autorización conforme a lo establecido en el MGSI.
- El acceso a las utilerías del sistema debe limitarse al mínimo de cuentas autorizadas. El acceso a las utilerías del sistema debe registrarse para facilitar la identificación de uso inapropiado. El uso de las utilerías del sistema no está permitido a menos que sea autorizado específicamente por el RSI.

6.2. Tiempo de Inactividad de Terminales.

- Después de un periodo de tiempo de inactividad de hasta 5 minutos, debe bloquearse el acceso a los servicios de información, así como depurar o eliminar la información visualizada en pantalla. Para desbloquear el acceso debe llevarse a cabo la re-autenticación a los servicios de información.
- Si la funcionalidad de limitar el tiempo de inactividad o el bloqueo de las terminales no está disponible en el sistema, debe forzarse al menos el empleo de protectores de pantalla con contraseñas.
- Cuando las máquinas del personal laboral pasen por largos periodos de tiempo sin atención, estas deben desconectarse (finalizar la sesión) o apagarse.

6.3. Límite de Tiempo de Conexión.

Las sesiones activas en los sistemas críticos deben limitarse a periodos de tiempo específicos.

6.4. Control de Acceso a la Aplicación.

- Las aplicaciones son utilizadas para facilitar procesos de negocio críticos que pueden contener información altamente sensible. El acceso no autorizado, inapropiado y mal intencionado a las aplicaciones sensibles puede dar como resultado acceso no autorizado a la información confidencial, modificaciones inapropiadas o pérdida de datos, y puede proveer información para posibles perpetradores que pudieran llevar a cabo actividades de fraude, entre otras. Por estas razones, el acceso a las aplicaciones debe ser robusto y altamente controlado.
- Las aplicaciones del Instituto FONACOT deben configurarse apropiadamente y sujetarse a controles de acceso para prevenir modificaciones o acceso no autorizado a los activos de información.

6.5. Restricción de Acceso a la Información.

- El acceso a las aplicaciones y a los datos contenidos en estas debe ser provisto de acuerdo con las necesidades y requerimientos reales de cada persona, su rol y función en el Instituto FONACOT.
- El acceso a las aplicaciones debe otorgarse considerando la adecuada segregación de funciones en los sistemas financieros y las responsabilidades funcionales.
- El control de acceso a las aplicaciones es soportado al menos por los siguientes principios:

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Restricción de menús basada en el mínimo privilegio.
- Restricción sobre el conocimiento que el personal puede tener o no, acerca de los recursos informáticos del Instituto.
- El acceso de lectura, escritura, borrado y ejecución deben asignarse de manera apropiada de acuerdo con la clasificación de información, rol y funciones inherentes al puesto o asignación.

6.6. Aislamiento de Sistemas Sensitivos.

Las aplicaciones sensitivas deben identificarse a través del proceso de evaluación de riesgos y separarse física y lógicamente de acuerdo con los requerimientos de información que impliquen especial manejo y protección.

6.7. Administración de Contraseñas.

- Los sistemas que administran el proceso por medio del cual se obliga al cumplimiento de los controles relativos a contraseñas para el acceso a la red, sistema operativo o aplicación, deben soportar los estándares del Instituto FONACOT respecto a la administración de contraseñas.
- Debido a que las aplicaciones y recursos de información del Instituto FONACOT son protegidos a través de los propios controles de acceso otorgados por contraseñas, debe aplicarse un estándar común en los diversos sistemas de administración de contraseñas con el que se garantice que la seguridad de los activos de información es aplicada de manera consistente.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3. POLÍTICA DE CRIPTOGRAFÍA.

1. INTRODUCCIÓN.

Esta política de seguridad tiene el objetivo de proporcionar los requerimientos mínimos para el uso y la administración de la tecnología de encriptación.

La filosofía de protección en cuanto al uso de encriptación es aplicar la tecnología para proteger activos informáticos de alto valor, minimizando varios riesgos a fin de cumplir con los requerimientos legales o reguladores, así como para proteger la reputación del Instituto FONACOT.

2. USO DE CIFRADO.

Los siguientes roles y responsabilidades en el uso y administración de tecnologías de encriptación se identifican en esta política.

- 1) Cada sistema de encriptación y de administración de llaves, en uso, debe tener asignado a una persona que sea el custodio de los activos. La persona que sea el custodio de los activos puede ser asignado para responsabilizarse de la operación y el mantenimiento de los sistemas de encriptación.
- 2) La persona que es el custodio de los sistemas de encriptación debe considerar los requerimientos de integridad y disponibilidad de las claves simétricas y asimétricas. Además, debe identificar la necesidad de archivar claves para habilitar el descifrado de la información encriptada con claves secretas.
- 3) La persona que es el custodio del activo aborda apropiadamente la segregación de funciones con base en los requerimientos para la protección de claves y la minimización de riesgos que se presentan por conceder privilegios excesivos.
- 4) La persona que es el custodio del activo provee procedimientos operacionales estándares y lineamientos para todos los aspectos de encriptación y administración, operación y mantenimiento de claves.
- 5) El RSI es el responsable de identificar los estándares de encriptación.
- 6) El RSI es el responsable de dar seguimiento al Análisis de Riesgos e implementación de controles de seguridad de la información.

2.1 Tratamiento de Datos Cifrados en equipo de cómputo.

El Instituto FONACOT a través del RSI determinará la estrategia sobre el cifrado de la información almacenada, procesada y transmitida por computadoras de escritorio y portátiles.

2.2 Cifrado de Mensajes de Correo Electrónico y Documentos Adjuntos.

La transmisión de correos electrónicos para entregas dentro del Instituto FONACOT que incluyen información clasificada como confidencial, ya sea en el cuerpo del mensaje o como archivo adjunto, debe estar protegida mediante encriptación. Resulta altamente recomendable habilitar la entrega de correos electrónicos seguros a direcciones externas al Instituto FONACOT, pero no es obligatorio.

Hasta que la encriptación de correos electrónicos y documentos adjuntos esté disponible para entregas fuera del Instituto FONACOT, el personal mediante pláticas de seguridad debe estar advertido sobre el riesgo de transmitir información confidencial a través del correo electrónico.

2.3 Cifrado de Datos e Información en Tránsito.

Cuando un sistema de aplicación transmite información confidencial, el uso de encriptación o hash de seguridad debe utilizarse cuando sea posible para asegurar la integridad de la información desde el punto de entrada hasta el punto de entrega, dentro y fuera de la red del Instituto FONACOT.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.4 Cifrado de Información Utilizada para la Autenticación.

El uso de la información utilizada para la autenticación de la identidad debe cubrir lo siguiente:

- Con excepción de la información de autenticación utilizada sólo una vez y que no puede ser reutilizada, ej.: contraseñas de una sola vez, la información para autenticar debe ser transmitida en una forma incomprensible o encriptada de emisor a receptor, para su transmisión.
- La información debe ser almacenada de manera que el contenido de la información no pueda ser determinada fácilmente, ej.: encriptación en un sólo sentido o como fragmentos hash. La información encriptada debe utilizar criptografía de un sentido, siempre que sea posible.

2.5 Uso de Certificados Digitales para la Autenticación.

Se deben utilizar certificados digitales y criptografía de claves públicas para ejecutar la autenticación en las tecnologías de autenticación que sean determinadas por el RSI.

2.6 Uso de Hash (verificación) de Seguridad.

El personal que custodia los activos pueden elegir el utilizar un hash de seguridad como mecanismo de integridad para archivos, mensajes o transmisiones. Un hash de seguridad se implementa utilizando la criptografía para claves públicas.

3. ADMINISTRACIÓN DE LLAVES.

Las llaves de encriptación simétrica y descifrado asimétrico, así como las llaves de firma, deben mantenerse secretas durante su ciclo de vida, de lo contrario las características de la protección de la tecnología de información son invalidadas.

Los algoritmos de encriptación y llaves deben ser suficientemente fuertes para que soporten un criptoanálisis, incluyendo ataques aleatorios y masivos dentro de un periodo satisfactorio de ataque.

El método de distribución y almacenamiento de llaves secretas debe ser suficientemente fuerte para que la clave no pueda ser comprometida durante la distribución o almacenamiento de esta.

3.1 Clasificación de Llaves.


Las llaves encriptadas deben ser clasificadas como información confidencial. Las llaves deben conservar su clasificación, es decir, no pueden ser degradadas durante su ciclo de vida.

3.2 Uso de Sistemas de Administración de Llaves Automatizadas.

El uso de sistemas de administración de llaves automatizadas prevé la seguridad de la distribución o intercambio de claves encriptadas. La distribución o el intercambio de llaves es el punto más débil de un sistema de encriptación y, por consiguiente, el más vulnerable a los ataques, dando como resultado llaves comprometidas.

El sistema de administración de llaves que en forma automática y segura generan y distribuyen nuevas llaves debe ser utilizado para todas las tecnologías de encriptación utilizadas dentro del Instituto FONACOT. La tecnología de distribución o intercambio de llaves debe ser un producto o tecnología estándar del Instituto FONACOT.

Si un sistema de administración de llaves automatizado no está en uso, los procedimientos operacionales estándar deben definir uno o más métodos de seguridad aceptables para la distribución o intercambio de llaves. En ningún caso, una llave encriptada debe distribuirse o intercambiarse durante una conversación telefónica, en un mensaje de correo electrónico, por fax no encriptado o por cualquier otro método que no forme parte de los métodos autorizados por los procedimientos operacionales estándar.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.3 Almacenamiento de Llaves y Barrido de Datos.

Los dispositivos de encriptación proveen un número de opciones para almacenamiento de llaves. Por ejemplo, las llaves pueden ser almacenadas en el disco duro del dispositivo, en la memoria o en una variedad de dispositivos periféricos o token.

La evaluación de riesgos debe abordar específicamente el riesgo para las llaves asociadas con el barrido de datos, basado en el método de almacenamiento, el nivel de clasificación de la información encriptada/descifrada utilizando la llave y el período de vida de la llave.

El RSI debe identificar un estándar para el almacenamiento de llaves de encriptación utilizadas para los siguientes propósitos:

- Llaves utilizadas para encriptar/descifrar información confidencial.
- Llaves utilizadas para encriptar/descifrar transferencia de fondos u otra transacción financiera.

3.4 Longitud de la Llave.

La longitud de la llave debe ser fija o variable de acuerdo con el algoritmo de encriptación. El RSI debe establecer estándares aceptables para la longitud de la clave con base en el algoritmo aplicable.

3.5 Vida de la Llave.

Cada llave debe tener un período de vida definido basado en la función de la llave y el riesgo asociado. Las consideraciones para establecer el período máximo de vida de la llave deben incluir la fuerza del algoritmo de encriptación y el método de almacenamiento.

4. ESTÁNDARES DE CIFRADO DEL INSTITUTO FONACOT.

El RSI debe identificar los estándares de encriptación utilizados dentro del Instituto FONACOT.

Los estándares de encriptación del Instituto FONACOT incluyen:

- Algoritmos de encriptación.
 - AES 128,256, 3 DES, RSA 2048.
- Sistema de administración de llaves.
 - HSM, RED HAT KEYSTORE.
- Longitud de llaves.
 - SSL 2048.
 - SSH 1024.
- Productos específicos de encriptación.
 - Symantec Endpoint Encryption, Thales Vormetric, Thales HSM, ESET End Point Encryption.
- Protocolos de red que utilizan servicios de encriptación.
 - IPSEC.

5. PROPIEDAD DE LOS SISTEMAS DE ENCRYPTACIÓN DEL INSTITUTO FONACOT.

Cada encriptación o sistema de administración de llaves en uso dentro del Instituto FONACOT debe tener asignado a una persona que sea el custodio del activo.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

4. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES.

1. INTRODUCCIÓN.

La operación diaria del Instituto FONACOT requiere la interconexión de áreas, personal laboral, sistemas y aplicaciones mismas que se realizan sobre la infraestructura tecnológica, debido a eso la configuración de red insegura puede proporcionar brechas en las conexiones, provocando el robo de información, transacciones electrónicas no autorizadas o facilitar amenazas ante personas maliciosas.

El propósito de esta política es proporcionar los lineamientos a seguir para la seguridad y protección en los activos de información propiedad del Instituto FONACOT, que son gestionados de manera digital a través de los sistemas de información, equipos tecnológicos, computadoras, redes, y otros dispositivos electrónicos que puedan conectarse a la red del Instituto FONACOT.

2. GESTIÓN DE SEGURIDAD EN LA RED.

2.1. Generalidades.

El Instituto FONACOT debe asegurar que las redes son administradas y controladas adecuadamente para estar protegidas contra amenazas, así como para mantener la seguridad de los sistemas y aplicaciones dentro de los mismos, incluyendo la información en tránsito.

Toda la infraestructura y los servicios en red del Instituto FONACOT debe ser instalada, respaldada y mantenida por el Departamento de Redes y Telecomunicaciones y/o proveedor de telecomunicaciones aprobado por el Instituto FONACOT.

2.2. Inventario de Red.

La DIT debe ser responsable de llevar un inventario actual de todos los componentes de red, sistemas, aplicaciones y activos de información asociados con la red.

2.3. Conexión de Sistemas a una Red.

Los activos informáticos propiedad del Instituto FONACOT, ejemplo: servidores, estaciones de trabajo, impresoras, copiadoras, etc., pueden ser conectados a la red siempre y cuando hayan sido configurados de acuerdo con los lineamientos de esta política y después de haber recibido aprobación de la DIT.

Todos los dispositivos que se conecten a una red del Instituto FONACOT deben registrarse con un identificador único, adicionalmente deben mantener una dirección de hardware (dirección MAC) que se pueda registrar y rastrear y utilizar.

Queda prohibida la conexión, desconexión, cambios de configuración o reubicación de recursos (dispositivos, tarjetas de acceso remoto, módems, routers o cualquier equipo) sin la correspondiente comunicación con el Departamento de Redes y Telecomunicaciones.

El acceso del personal y terceros a las redes del Instituto FONACOT debe seguir los lineamientos establecidos en la Política de Control de Accesos.

2.4. Expansión de Redes.

La persona Titular del Departamento de Redes y Telecomunicaciones debe considerar los riesgos asociados, controles a implementar, requerimientos de conexión y los protocolos de comunicación que sean necesarios durante cualquier expansión de la red, con la finalidad de asegurar la continua protección de la red y la información almacenada, procesada y transmitida a través de esta.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.5. Planeación de la Capacidad.

Los operadores de redes deben ser responsables de monitorear la utilización de la red, pronosticar necesidades futuras y comunicar estos pronósticos en un plan anual de capacidad a la SGTIC, quien debe revisar las capacidades y la disponibilidad adecuada de los servicios de red.

2.6. Uso de Redes Inalámbricas.

Todo el personal laboral o externo que se conecte a la red inalámbrica debe hacerlo por medio de una cuenta y contraseña del dispositivo inalámbrico, adicionalmente el personal debe estar autorizado para acceder a la red por medio de la dirección MAC del equipo.

Todos los dispositivos de infraestructura inalámbrica que se conectan a una red o proporcionen acceso a la red del Instituto FONACOT deben:

- Utilizar el protocolo de autenticación extensible: autenticación rápida mediante túnel seguro (EAP-FAST), protocolo de autenticación extensible protegido (PEAP) o protocolo de autenticación extensible-seguridad de la capa de traducción (EAP-TLS) como protocolo de autenticación.
- Utilizar el Protocolo de integridad de clave temporal (TKIP) o Sistema de cifrado avanzado (AES) con una longitud mínima de clave de 256 bits.
- Cambiar el nombre SSID y contraseña predeterminada.
- De usar WPA2-PSK, se debe configurar una clave secreta compleja (al menos 20 caracteres) en el cliente inalámbrico y el punto de acceso inalámbrico.
- No se permite el uso de los dispositivos Bluetooth como transferencia de información dentro del Instituto FONACOT.

2.7. Seguridad de la Transmisión.

Se debe proporcionar confidencialidad e integridad durante la transmisión, de la información clasificada como confidencial, utilizando tecnología de encriptación revisada por el Departamento de Redes y Telecomunicaciones. Esto aplica a la transmisión entre redes del Instituto FONACOT, así como con terceras partes. La seguridad en la transmisión de la información confidencial y reservada deben aplicarse los siguientes principios:

- La seguridad de la transmisión a través de líneas contratadas o redes públicas que conectan elementos de la red interna puede depender de medidas, ejemplo: herramientas de encriptación, bajo el control de un proveedor de servicios. En este caso, el acuerdo contractual con el proveedor de servicios debe cumplir con los requisitos de la Política de Relación con Terceros.
- La seguridad de la transmisión realizada por redes IP públicas que conectan elementos de redes debe ser proporcionada por tecnología de VPN.
- La seguridad de la transmisión para conexiones a través de redes públicas debe estar protegida de manera apropiada por productos o tecnologías estándares, aprobadas por el RSI.
 - La transmisión de los datos debe ser de manera cifrada y siguiendo los lineamientos de la Política de Criptografía.

Las VPN que establecen una conexión externa deben cumplir con los requisitos de la Política de VPN de las conexiones externas. Las VPN que se establecen o los elementos de un servicio de acceso remoto deben cumplir con los requisitos de los servicios de acceso remoto y deben emplear tecnología de cifrado.

2.8. Seguridad en los Servicios de Red.

Las evaluaciones de riesgo deben proporcionar una definición clara de los atributos de seguridad de cualquier servicio de red proporcionado por una red, dentro del alcance de la evaluación.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.9. Control del Enrutamiento de Red.

El Instituto FONACOT debe resguardar la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

Los controles de enrutamiento deben ser implementados en los límites entre redes que tienen diferentes activos, así como en las principales conexiones. Deben basarse en mecanismos de revisión de direcciones de origen y destino positivos. En particular, el tráfico que sale de una red debe estar controlado para asegurar que las direcciones IP fuente están dentro del rango IP de la red.

La forma en que los controles de enrutamiento se aplican debe ser documentada y estar disponible a otros activos de la red. Los controles de enrutamiento de red pueden ser implementados en software o hardware.

El enrutamiento límite entre el Instituto FONACOT y un tercero debe ser estático o realizarse mediante un mecanismo controlado (es decir, un mapa de rutas o una política de redistribución de rutas controladas por el Instituto FONACOT).

3. TRANSFERENCIA DE INFORMACIÓN.

La información digital en movimiento debe ser transmitida y/o transportada por la red interna por el Instituto FONACOT, mediante los equipos de seguridad perimetral del Instituto FONACOT, teniendo como mínimo los equipos de firewall, switch, equipo de filtrado web.

3.1. Políticas y Procedimientos de Transferencia de Información.

El Instituto FONACOT define políticas en la transferencia de información que se envía de forma interna o externa a proveedores o clientes que se describen a continuación.

3.2. Transferencia de Información a Proveedores o Clientes.

- El canal de comunicación para el intercambio de información electrónica autorizada por el Instituto FONACOT es el correo electrónico del Instituto FONACOT.
- Se debe evitar el envío de información sensible o crítica a personal externo del Instituto FONACOT. La transmisión de información sensible o crítica a personal externo debe ser únicamente por las actividades laborales que así lo requieran y por los medios autorizados por el Instituto FONACOT.
- El personal externo debe contar con convenio de confidencialidad y acuerdo de transferencia de la información mediante el contrato establecido entre el Instituto FONACOT y terceros.

3.3. Transferencia de Información Digital o Electrónica.

- El Instituto FONACOT cuenta con un repositorio de información que debe dar acceso únicamente al personal autorizado.
- Se deben definir las herramientas para el envío de información de uso interno, mismos que deben contar con mecanismos de acceso y privilegios.
- La transferencia de información digital debe ser utilizando mecanismos de autenticación y protocolos de cifrado o seguros como FTPS, HTTPS, SSL o TLS.

3.4. Transferencia de Información Física.

La información de uso interno debe ser enviada por los mecanismos autorizados por el Instituto FONACOT:

- Entrega de información física en la mano del receptor.
- Proteger la información utilizando un sobre cerrado, sin referencias sobre su contenido.
- Elaborar un contra recibo por toda la información enviada de manera física, para verificar la recepción de la información.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.5. Acuerdos de Transferencia de Información.

Cuando la información física o electrónicamente del Instituto FONACOT es intercambiada con otra organización, estas deben crear un acuerdo que proteja la información en tránsito sobre pérdida, divulgación y daño, de acuerdo con la clasificación de información y la naturaleza de la relación de negocio. El acuerdo de la contraparte al menos contendrá:

- Declaraciones.
- Obligaciones y responsabilidades.
- Vigencias.
- Incumplimientos.

3.6. Mensajería por Aplicaciones Móviles y Redes Sociales.

No está permitido el envío de ningún tipo de información relacionada con el Instituto FONACOT a través de aplicaciones móviles y/o redes sociales, los anterior haciendo uso de cuentas no oficiales o cuentas personales. Cualquier excepción debe ser solicitada por la Dirección de la Unidad Administrativa correspondiente y aprobada por el RSI.

3.7. Acuerdos de Confidencialidad y no Divulgación.

La confidencialidad debe abordarse en todos los acuerdos contractuales. Los términos de los acuerdos de confidencialidad deben ser revisados cuando los términos del contrato hayan cambiado.

Dentro de los acuerdos de confidencialidad se deben tener en cuenta los siguientes aspectos:

- Definir la información a proteger.
- Duración esperada del acuerdo.
- Términos para destruir o devolver la información cuando termine el acuerdo.
- Acciones esperadas que deben adoptarse en caso de incumplimiento de este acuerdo.

Los acuerdos de confidencialidad y no divulgación deben revisarse periódicamente y cuando se produzcan cambios que influyan estos requisitos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

5. POLÍTICA DE DESARROLLO SEGURO.

1. INTRODUCCIÓN.

Esta política tiene el propósito de definir y establecer los requisitos mínimos para la seguridad de desarrollo de software, integración de sistemas y mantenimiento de actividades de sistemas.

Los principales elementos de protección requeridos por esta política son:

- Los requisitos para la aplicación y seguridad de sistemas deben de ser abordados en las etapas tempranas de los análisis de requisitos.
- Debe haber una separación estricta entre el desarrollo, prueba y los ambientes operacionales. A los desarrolladores de sistemas no se les debe otorgar el acceso a ambientes operacionales.
- La documentación apropiada es requerida para todas las actividades de desarrollo con requisitos de seguridad.
- La administración del control/configuración de cambios debe ser implementada en todos los ambientes de desarrollo.

2. REQUISITOS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN.

2.1 Políticas Generales.

La SDSI debe asegurarse de cumplir con las siguientes directrices en sus aplicaciones generadas por el Instituto FONACOT o por las aplicaciones generadas por terceros.

- Toda aplicación debe llevar a cabo un proceso de autenticación que asegure la identificación de manera única del personal que accede a la información y aplicaciones.
- Toda aplicación debe permitir controlar el acceso a la información mediante roles, perfiles o funciones.
- Toda la gestión de información confidencial debe ser tratada conforme a la Política de Gestión de Activos de Información, dicha información debe permanecer cifrada durante su almacenamiento y transporte.
- Toda aplicación debe llevar a cabo un registro de auditoría, que contenga el detalle de las actividades realizadas.

2.2 Análisis y Especificación de los Requisitos de Seguridad.

Los requisitos de seguridad deben ser abordados durante la etapa del análisis de requisitos para la planeación del proyecto. La persona que sea custodio del activo, debe ser responsable y ponerse a cargo del cumplimiento del desarrollo del proyecto y de la nueva aplicación/sistema, con las políticas y estándares del Instituto FONACOT.

2.2.1 Etapa de Análisis.

Para minimizar el riesgo de fallas del sistema, resultando en no disponibilidad o pérdida de información, la preparación y planeación a futuro se realiza mediante una revisión funcional / técnica de los cambios a implementar, con la finalidad de eliminar impactos a procesos críticos del Instituto FONACOT.

Los criterios de aceptación para software y sistemas integrados deben ser establecidos para abordar los requisitos de seguridad y asegurar que las pruebas apropiadas sean desarrolladas. La persona que sea custodio de activo. debe aceptar formalmente los sistemas y los cambios a sistemas existentes previos al despliegue del sistema o del cambio.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.3 Servicios de Aplicaciones Seguras en Redes Públicas.

Para el acceso a los ambientes de desarrollo y preproducción fuera de oficina, siempre debe realizarse por medio de una VPN, misma que debe tramitarse por el personal que así lo requiera.

2.4 Protección de Aplicaciones de Servicios Financieros.

Para intercambio de información con externos, se utilizan método de cifrado y canales seguros.

3 REQUISITOS EN DESARROLLO Y PROCESOS DE SOPORTE.

3.1 Política de Desarrollo Seguro.

El Instituto FONACOT se asegura del desarrollo interno o externo de los sistemas de información en cumplimiento con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

Además, asegura que todo software desarrollado o adquirido, interna o externamente cuenta con las patentes o licencias requeridas para su uso y soporte requerido.

Toda aplicación desarrollada debe llevar a cabo un proceso de autenticación que asegure la identificación de la persona que accede a las aplicaciones e información.

Toda aplicación desarrollada debe permitir controlar el acceso a la información mediante roles, perfiles o funciones.

Tener un registro de auditoría que contenga la actividad realizada por la persona.

Se debe tener en cuenta en las siguientes características que debe contener la aplicación:

- Autenticación.
- Implementación de https.
- Evasión de autenticación.
- Autenticación la persona.
- Complejidad de contraseñas.
- Renovación de contraseñas.
- Autorización:
 - Manejo de los parámetros de autorización – Separación de funciones.
 - Acceso a páginas o funciones restringidas.
 - Flujo de trabajo de la aplicación.
- Integridad de la Entrega de Información:
 - Cifrado del canal y de la información confidencial que es transportada.
 - Administración de ambientes:
 - Separación y homologación de ambientes.
- Desarrollo:
 - Uso de Diccionario de Datos.
 - Uso de Técnicas Estructuradas.
 - Estándares de Programación.
 - Estándares de Documentación.
 - Parámetros de Proceso.
 - Ejecución de programas con el mínimo nivel de privilegios para realizar la tarea.
 - Uso de lenguajes para prevenir el buffer overflow (Perl, Java, .net).

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

El RSI se encarga de validar con las respectivas áreas el cumplimiento de lo siguiente:

- El código fuente sin ofuscar, debe ser entregado al Instituto FONACOT.
- Las diferentes versiones del código de aplicaciones / software debe estar incluido en un repositorio indicado por el Instituto FONACOT.
- Las pruebas de seguridad deben ser ejecutadas por equipos diferentes a los equipos que desarrollaron la solución, el Instituto FONACOT debe asegurar que haya segregación de funciones y que no existan conflictos de interés.
- Todo código fuente debe ser inspeccionado o certificado que está libre de código oculto, código malicioso e intenciones maliciosas. En algunos casos, el proveedor que provee el código fuente puede certificar su propio software y la reputación del proveedor debe ser evaluada como parte de la aceptación del software.
- La aplicación debe contar con:
 - Mecanismos o esquemas de seguridad de la información.
 - Política de privacidad y protección de datos personales, de conformidad con la legislación aplicable.
 - Perfiles de la persona.
 - Matriz de trazabilidad.
 - Mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma), cuando resulte aplicable.
 - Garantizar que el acceso a las plataformas digitales de páginas web se realice a través de mecanismos de autenticación y cifrado mediante certificados digitales.

3.2 Procedimiento de Control de Cambios a Sistemas.

Los cambios a los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios. Esto se hace a través del procedimiento de control de cambios a sistemas que consta de las siguientes actividades:

- Registrar el cambio (herramienta HEAT/iTop) bajo procedimiento de control de cambios.
- Preanálisis del cambio.
- Diseño de la solución.
- Desarrollo de la solución.
- Pruebas de calidad.
- Reunión de comité de cambios.
- Despliegue a producción.

3.3 Revisión Técnica de Aplicaciones Después de Cambios en la Plataforma de Producción.

Una vez realizados los cambios para el despliegue del sistema desarrollado o adquirido de acuerdo con el procedimiento de control de cambios, se debe:

- Probar la aplicación para comprobar que efectivamente permanecen las medidas de protección requeridas.
- Las pruebas se llevan a cabo por los solicitantes del cambio o mantenimiento; las pruebas no se deben realizar por el mismo personal que generó el cambio.
- Generar la matriz de casos de pruebas que cubra con el alcance solicitado y afectado.
- Todos los casos de prueba deben ser probados y concluidos de forma exitosa, para que se pueda otorgar el Vo. Bo. para la liberación a producción.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.4 Restricción en los Paquetes de Software.

- Los paquetes de software sólo deben ser modificados por el personal autorizado para esta actividad y debe existir una solicitud de por medio.
- Todo cambio a sistemas de información o software debe apegarse al procedimiento de gestión de cambios.
- Cuando la persona que es el custodio de activo determine que un cambio (nueva programación) en el software es esencial, debe documentar lo siguiente:
 - Análisis de impactos en procesos de negocio (documento de entendimiento).
 - Preanálisis del requerimiento.
 - Vo. Bo. de los interesados en el cambio.
 - Para cualquier cambio, se debe tener un control de versiones para el código a modificar / implementar.

3.5 Principios de Ingeniería en Sistemas Seguros.

Todos los desarrollos internos, externos, adquisiciones de sistemas y aplicaciones deben someterse a pruebas técnicas donde se revisa la validación de datos y mecanismos de autenticación, etc.

Los principios que se deben tomar en cuenta son:

- Implementar medidas de seguridad al sistema en desarrollo, para satisfacer los objetivos de seguridad del Instituto FONACOT.
- Proteger la información utilizada por el sistema en desarrollo, mientras está siendo procesada, en tránsito y en almacenamiento.
- Usar únicamente los lenguajes y versiones autorizados por el Instituto FONACOT.
- Implementar tecnología, hardware, firmware y software de confianza.
- Limitar el acceso a la operatividad que permitan activar y desactivar funciones de seguridad del sistema o cambiar los privilegios de las cuentas o programas.
- Identificar y prevenir errores comunes, evitar el uso de tecnología o componentes vulnerables.
- Identificar requerimientos y en su caso, implementar tecnologías que permitan la alta disponibilidad, replicación o sincronización de información.

3.6 Entorno de Desarrollo Seguro.

Se deben controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Se debe resguardar por la seguridad del proyecto o del entorno de soporte. Se debe garantizar que todas las propuestas de cambio en los sistemas son revisadas para validar que no comprometen la seguridad del sistema o del entorno operativo.

Se debe incorporar la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema.

3.7 Desarrollo de Sistemas Subcontratado.

Cuando el desarrollo del software ha sido tercerizado, la persona que es el custodio del activo debe abordar lo siguiente, aparte de los requisitos establecidos en la Política de Relación con Terceros.

- Abordar completamente cualquier acuerdo aplicable de licencia, código de posesión y problemas de DPI.
- El área requirente de la contratación debe asegurar que en las cláusulas del contrato se incluyan acuerdos para mantener el diseño y código del sistema en custodia por parte del Instituto FONACOT,

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

para permitir llevar a cabo el mantenimiento del sistema en caso de que el proveedor se vuelva incapaz de cumplir con sus obligaciones de garantía y otras obligaciones de mantenimiento.

El RSI da seguimiento al cumplimiento de los siguientes puntos:

- El código fuente sin ofuscar, debe ser entregado al Instituto FONACOT.
- Las diferentes versiones del código de aplicaciones/software debe estar incluido en un repositorio indicado por el Instituto FONACOT.
- Las pruebas de seguridad deben ser ejecutadas por equipos diferentes a los equipos que desarrollaron la solución, el Instituto FONACOT debe asegurar que haya segregación de funciones y que no existan conflictos de interés.
- Todo código fuente debe ser inspeccionado o certificado que está libre de código oculto, código malicioso e intenciones maliciosas. En algunos casos y de común acuerdo, el proveedor que provee el código fuente puede certificar su propio software y la reputación del proveedor debe ser evaluada como parte de la aceptación del software.
- La aplicación/software debe contar con lo siguiente:
 - Mecanismos o esquemas de seguridad de la información.
 - Política de privacidad y protección de datos personales, de conformidad con la legislación aplicable.
 - Perfiles de la persona.
 - Matriz de trazabilidad.
 - Mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma), cuando resulte aplicable.
 - Garantizar que el acceso a las plataformas digitales de páginas web se realice a través de mecanismos de autenticación y cifrado mediante certificados digitales.

3.8 Pruebas de Seguridad a los Sistemas.

Al realizar las pruebas se deben llevar a cabo los siguientes puntos:

- Los datos de pruebas pueden ser de los siguientes tipos:
 - Datos Reales.
 - Datos Ficticios.
- Generar los archivos en equipos y áreas diferentes al de producción, con solo la información que es requerida.
- Las áreas y equipos de pruebas deben contar con controles de acceso, para que solo el personal autorizado pueda acceder y utilizar esta información.
- El área de desarrollo realizará las pruebas unitarias correspondientes a las funcionalidades, antes de ser entregado a los demás ambientes y debe registrar los resultados de estas.
- El área usuaria solicitante del cambio debe definir y ejecutar todas las pruebas concernientes a la funcionalidad afectada.

3.9 Pruebas de Aceptación a los Sistemas.

De acuerdo con el alcance de las pruebas, se generan los conjuntos de datos correspondientes que cubren todas las casuísticas relacionadas con la funcionalidad afectada.

El área solicitante del cambio es la única facultada para dar Vo. Bo. de la funcionalidad modificada.

3.10 Contraseñas en Desarrollo Seguro de Aplicaciones.

- Los desarrolladores de aplicaciones deben asegurarse de que sus programas contengan las siguientes precauciones de seguridad:

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01 Vigencia: Julio, 2024	
--	--	--	---

- Las aplicaciones deben realizar la autenticación de cada persona de manera individual.
- Las aplicaciones no deben almacenar contraseñas en texto claro o en cualquier forma fácilmente reversible.
- Las aplicaciones no deben transmitir contraseñas en texto claro a través de la red.
- Las aplicaciones deben proporcionar algún tipo de gestión de roles, de modo que la persona pueda asumir las funciones de otra sin tener que conocer su contraseña.

4 DESARROLLO DE SOFTWARE POR TERCEROS BAJO CONTRATO CON EL INSTITUTO FONACOT.

La SDSI debe asegurarse que los proveedores implementen los controles necesarios para mitigar los riesgos descritos que proveen las instituciones como el OWASP Top 10 y el SANS Top 25.

4.1 Análisis de Vulnerabilidades.

El proveedor debe realizar las pruebas necesarias basándose en el Top 10 de OWASP y el Top 25 de SANS para poder determinar el despliegue de la aplicación al ambiente productivo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

6. POLÍTICA DE RELACIÓN CON TERCEROS.

1. INTRODUCCIÓN.

Esta política tiene el propósito de establecer los lineamientos que regulan los aspectos de vigilancia y cumplimiento para los proveedores de tecnologías de la información.

2. RELACIÓN CON TERCEROS.

2.1 Lineamientos de Vigilancia y Cumplimiento para los Proveedores Críticos del Instituto FONACOT.

Las actividades de vigilancia, cumplimiento y desempeño para la gestión de los proveedores críticos de tecnologías de la información en el Instituto FONACOT deberán sujetarse a los siguientes Lineamientos.

a) Lineamientos para las restricciones o condiciones, respecto a la posibilidad de que el tercero subcontrate, de manera parcial o total la prestación del producto o servicio.

El Instituto FONACOT validará que los proveedores de tecnologías de la información cumplan con las restricciones que impidan que estos subcontraten con un tercero los servicios de su responsabilidad. Para esto, los administradores de los contratos en materia de Tecnologías de la Información deberán validar los siguientes aspectos

- El cumplimiento a las restricciones de subcontratación de los servicios a un tercero, conforme a lo estipulado en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y al Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamiento y Servicios del Instituto FONACOT.
- Que la prohibición de subcontratación esté regulada y condicionada en los propios contratos que se celebren con los proveedores en términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público para lo cual se deberá verificar que, dentro de las cláusulas de los contratos, se especifique de manera explícita la restricción respecto a la subcontratación parcial o total de los productos y/o servicios objeto de los contratos.

b) Lineamientos para la confidencialidad y seguridad de la información de los clientes del Instituto FONACOT.

El Instituto FONACOT debe salvaguardar la confidencialidad y seguridad de la información de sus clientes con base a lo estipulado en la Ley Federal de Transparencia y Acceso a la Información Pública, así como en Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Los administradores de los contratos están obligados a verificar que establezcan cláusulas de salvaguarda correspondientes para garantizar la confidencialidad y seguridad de la información de los clientes del Instituto FONACOT. De manera adicional, la SGTIC mediante sus áreas internas deberá dar seguimiento al cumplimiento del presente lineamiento, y en caso de identificar algún incumplimiento, deberá efectuar el cálculo preliminar del monto de la penalización y notificar a la Dirección de Recursos Materiales y Servicios Generales, para que informe por escrito al proveedor el cálculo de la pena convencional, indicando el número de días de atraso, así como la base para su cálculo y el monto a que se hizo acreedor.

c) Lineamientos para las obligaciones del Instituto FONACOT y del tercero, así como el procedimiento para vigilar su cumplimiento y en su caso, las consecuencias legales al presentarse algún evento de incumplimiento y desempeño.

Los administradores de los contratos en materia de tecnologías de la información deberán revisar y vigilar el cumplimiento de los compromisos establecidos en los contratos, con base en los siguientes aspectos:

- Que se dé cumplimiento a lo estipulado en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- De manera particular, se deberán considerar:
 - Las restricciones o condiciones, respecto a la posibilidad de que el tercero subcontrate, de manera parcial o total la prestación del producto o servicio.
 - La confidencialidad y seguridad de la información de los clientes del Instituto FONACOT.
 - Las condiciones que deben cumplir los productos y servicios, calidad y tiempos de entrega.
- Los contratos deben indicar las causales de rescisión y/o el procedimiento de rescisión administrativa, considerando lo siguiente
 - Incumplimientos.
 - Retrasos en el servicio.
 - Entrega de servicio parcial o deficiente, así como lo correspondiente con la procedencia de los pagos y penas convencionales o deductivas.

d) Lineamientos para los mecanismos de solución de disputas en contratos de productos y/o servicios.

En la solución de disputas de contratos con proveedores de tecnologías de la información, el Instituto FONACOT utilizará los mecanismos sustentados y normados mediante lo siguiente:

- Las soluciones de disputas se realizarán conforme a lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- El arbitraje y los mecanismos de solución de controversias deben estar basados en el procedimiento de conciliación, ante la Secretaría de la Función Pública y/o Tribunales Federales Competentes.

e) Lineamientos para los planes de continuidad del negocio y procedimientos de contingencia en caso de desastres.

Con relación a los productos y/o servicios que estén relacionados con activos críticos del Instituto FONACOT y que sean provistos por un tercero a través de un contrato administrativo, los administradores de los contratos deberán verificar que en los contratos se establezca el reconocimiento y compromiso por parte del tercero, de que dispone de la capacidad técnica y operativa para responder ante una contingencia o incidente imprevisto que podría afectar la continuidad del negocio del Instituto FONACOT.

De manera particular, se deberá verificar que, en el anexo técnico de los contratos, estén incluidas las siguientes condiciones:

- Niveles de servicio.
- Niveles de operación.
- Niveles de redundancia.
- Planes de continuidad de la operación.
- Grado de intermitencia permitido en el servicio.
- Tiempos de respuesta.

En caso de incumplimiento se deben ejecutar los lineamientos correspondientes a los mecanismos de solución de disputas en contratos de productos y/o servicios, mismos que se encuentran en el inciso d) de esta sección.

f) Lineamientos para el uso y explotación a favor del Instituto FONACOT sobre las bases de datos producto de los servicios.

Según el tipo de servicio contratado, los administradores de contratos deberán verificar que en los Anexos Técnicos existen los términos y condiciones relacionados con el uso y explotación a favor del Instituto FONACOT, sobre las bases de datos producto de los servicios prestados.

De manera particular, el Anexo Técnico deberá contener obligaciones, que garanticen el uso y explotación a favor del Instituto FONACOT, sobre las bases de datos producto de los servicios.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.2 Requisitos Generales de Seguridad de la Información con Terceros.

El Instituto FONACOT establecerá en los contratos y Anexos Técnicos lo siguiente:

- Definir las funciones y responsabilidades con respecto a la seguridad de la información.
- Aspectos de la propiedad, divulgación o cualquier otra acción relacionada con la información del Instituto FONACOT.
- Debe mantenerse la información vigente conforme a los términos de las Leyes aplicables.

El área requirente se asegurará que en el Anexo Técnico se incluya según sea necesario, lo siguiente:

- El apego al MGSÍ del Instituto FONACOT.
- Realizar la gestión de cuentas conforme a la Política de Control de Accesos y al Procedimiento de Gestión de Cuentas.
- Gestión de activos conforme a la Política de Gestión de Activos de Información.
- En cuanto a los servicios, los contratos deben tener objetivos para el servicio proporcionado, SLA, OLA, criterios de desempeño y planes para reportar el desempeño.
- Niveles de servicio, niveles operativos establecidos, la aplicación de penas convencionales, en caso de incumplimiento.
- Controles físicos y lógicos que se utilizan para restringir y delimitar el acceso a la información sensible del Instituto FONACOT.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres (DRP, pólizas de servicio, etc.).
- Responsabilidades respectivas de cada una de las partes involucradas, tanto en operaciones cotidianas como en escenarios de contingencia.
- Proceso de respuesta a incidentes en donde se indiquen los niveles de servicio, de soporte y escalamiento de problemas e incidencias.
- Proceso de Gestión de cambios, e interacciones con otros procesos.
- Controles para asegurar la protección contra software malicioso, según sea necesario conforme a lineamientos indicados en la Política de Protección contra Malware.
- Procedimiento de borrado seguro conforme a la Política de Seguridad Física de la Información.

2.3 Eliminación de Accesos a la Infraestructura Informática y Devolución de Activos.

Cuando se modifica o finaliza el vínculo contractual con un tercero, el administrador del contrato por parte del Instituto FONACOT debe proceder con la solicitud de la baja para la eliminación de accesos, borrado seguro y la devolución de los activos (si aplica).

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

7. POLÍTICA DE SEGURIDAD EN LAS OPERACIONES.

1. INTRODUCCIÓN.

Contar con los documentos de apoyo para asegurar la continuidad de las mejores prácticas desarrolladas por el Instituto FONACOT para sus operaciones y administración del día con día.

Adicionalmente, se evalúa el posible impacto operativo de los cambios previstos a sistemas y equipamiento, verificar su correcta implementación, asignando las responsabilidades correspondientes para administrar los medios técnicos necesarios que permitan la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad, es necesario monitorear la capacidad de los sistemas en operación y proyectar los requerimientos a futuro.

El control de la realización de las copias de resguardo de información, así como la prueba semestral de su restauración, permite garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada área.

Se define y documenta controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes del Instituto FONACOT.

Finalmente, se verifica el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

2. PROCEDIMIENTOS Y RESPONSABILIDADES.

2.1. Procedimientos Operativos Documentados.

El Instituto FONACOT cuenta con procedimientos tecnológicos, mismos que deben ser verificados y/o actualizados por lo menos una vez al año.

2.2. Gestión del Cambio.

El Instituto FONACOT debe controlar los cambios que surjan, procedimientos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información a través un procedimiento de gestión del cambio.

Los cambios deben realizarse tomando en cuenta lo siguiente:

- Todos los cambios que se pretendan realizar en los sistemas tecnológicos del Instituto FONACOT deben estar documentados.
- Los cambios deben ser propuestos por el personal del Instituto FONACOT. En caso de que el cambio sea propuesto por un tercero, el personal encargado de la administración del servicio debe ser quien realice la propuesta del cambio ante el Instituto FONACOT.
- Los cambios deben ser notificados al RSI, para identificar y evitar posibles consecuencias negativas sobre la seguridad de la información.
- Se debe disponer de planes de emergencia que permitan la recuperación de la última configuración estable antes del cambio, este plan debe estar descrito en el documento de la solicitud del cambio.
- La aprobación del cambio la tiene que realizar el RSI.
- La DTI y la DIT son los responsables de verificar que los cambios se hayan implementado correctamente y que no exista una afectación en la operación del Instituto FONACOT.
- Todos los cambios deben ser solicitados por medio de correo electrónico y asignarse en un ticket en la mesa de servicio, con la finalidad de tener la trazabilidad del cambio.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Para la implementación de un cambio de emergencia derivado de un incidente de ciberseguridad, esté se debe aplicar a la brevedad únicamente con la autorización del RSI.

2.3. Gestión de Capacidad.

El Instituto FONACOT debe asegurar el desempeño y capacidad de la plataforma tecnológica de manera anual.

El responsable de los servicios de infraestructura debe realizar el monitoreo anual que debe considerar:

- Consumo de recursos de procesadores, memorias, discos.
- Ancho de banda, internet y tráfico de las redes de datos.

2.4. Separación de Entornos de Desarrollo, Prueba y Producción.

Los entornos de desarrollo, pruebas y producción deben de separarse para reducir los riesgos de accesos o cambios no autorizados en el entorno.

Para el entorno de desarrollo se debe tomar en cuenta:

- IP para ingreso o dominio (dirección IP).
- Mecanismo de separación (servidor físico o virtual).
- Mecanismo de identificación (despliegue de mensaje de alerta).
- Características de seguridad de acceso (perfiles de acceso, segregación de módulos, segregación de redes).
- Características de seguridad de código fuente (mecanismos de seguridad del repositorio que contiene el código fuente, librerías, etc.).

Para el entorno de pruebas se debe tomar en cuenta:

- IP para ingreso o dominio (dirección IP).
- Mecanismo de separación (servidor físico o virtual).
- Mecanismo de identificación (despliegue de mensaje de alerta).
- Características de seguridad de acceso (perfiles de acceso, segregación de módulos, segregación de redes).
- Tipo de datos de prueba (reales y ficticios).
- Características de seguridad para datos pruebas.

Para el entorno de producción se debe tomar en cuenta:

- IP para ingreso o dominio (dirección IP).
- Mecanismo de separación (servidor físico o virtual).
- Mecanismo de identificación (despliegue de mensaje de alerta).
- Características de seguridad de acceso (perfiles de acceso, segregación de módulos, segregación de redes).
- Personal laboral autorizado para hacer modificaciones en el entorno (roles autorizados).

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3. RESPALDOS.

3.1. Copias de Seguridad de la Información.

Se deben de crear copias de seguridad para todos los sistemas declarados como críticos para el Instituto FONACOT con la finalidad de velar por la continuidad del negocio.

El RSI del Instituto FONACOT, debe asegurar que la información crítica, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su confidencialidad, identificación, protección, integridad y disponibilidad.

3.2. Requerimientos de Respaldo en Evaluaciones de Riesgo.

Las evaluaciones de riesgo de aplicaciones deben considerar la disponibilidad de los medios de respaldo en caso de falla de sistemas o componentes. Las evaluaciones de riesgo deben considerar la suficiencia de los requerimientos del MGSI y cualquier necesidad de medidas más fuertes, tales como la producción de dos respaldos, con un conjunto en el centro de datos principal y otro enviado a otra ubicación.

3.3. Horario de Respaldos.

El Instituto FONACOT debe establecer y mantener un horario de actividades de respaldo para cada servidor, donde especifique las aplicaciones e información almacenada o asociada.

Este horario debe ser registrado diariamente por los operadores responsables de ejecutar y administrar los resultados de los medios de almacenamiento y respaldos.

3.4. Requerimientos para Respaldos Especiales.

Los respaldos fuera de ciclo son cualquier respaldo que no está programado de manera regular. Un respaldo fuera de ciclo debe realizarse con base en lo siguiente:

- Se debe realizar un respaldo completo del sistema de archivos antes y después de la instalación del sistema operativo que se haya adquirido.
- Se debe realizar un respaldo parcial antes y después de la instalación de cualquier aplicación adquirida, esto incluye todos los archivos y directorios que afecten la instalación.
- Se debe realizar un respaldo parcial después de la instalación de una base de datos, incluyendo todas las nuevas estructuras de datos.

Los respaldos fuera de ciclo se deben retener en sitio por lo menos 5 días laborales para su uso en actividades de restauración.

3.5. Respaldos por Evento o Calendario.

Es posible que las aplicaciones requieran un respaldo basado en la ocurrencia de algún evento, respaldo trimestral, de fin de mes o de fin de año. El personal que custodia los activos con requerimientos específicos de respaldo basados en eventos o en la programación deben proveer instrucciones escritas a la SSOS detallando esos requerimientos con los requerimientos de retención asociada para los medios de respaldo. Los medios producidos, como resultado de alguna solicitud del personal que custodia los activos, deben ser almacenados fuera de las instalaciones.

3.6. Respaldos de Laptops.

Los respaldos de software o la información almacenada en una computadora portátil es la responsabilidad de cada persona a quien le fue asignado el equipo. La SSOS debe identificar un periférico apropiado para producir algún medio removible como el dispositivo de respaldo. El personal debe ser capacitado sobre la realización de respaldos y la protección de medios removibles.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.7. Protección de Copias de Respaldos.

3.7.1. Clasificación de los Medios de Respaldo.

Los medios removibles de almacenamiento considerados para el respaldo de la información del Instituto FONACOT tales como discos duros, memorias USB, cintas magnéticas o los CD-ROM deben ser clasificados como confidenciales. Los medios de respaldo deben estar protegidos contra escritura. Todo medio considerado de respaldo debe estar adecuadamente etiquetado.

3.7.2. Almacenamiento Fuera de Línea de Datos Respaldados.

Los medios de respaldo removibles deben ser almacenados en un complejo fuera de las instalaciones, asegurados con base en los siguientes requerimientos:

- Si se realizan respaldos parciales, el último respaldo completo de la semana, así como los respaldos de días previos, deben ser retenidos en las instalaciones y almacenados en un contenedor a prueba de fuego. Estos respaldos, deben ser rotados al complejo de almacenamiento fuera de las instalaciones para ser conservados por lo menos 30 días.
- Si se realizan respaldos completos, los medios del respaldo de un día anterior deben ser retenidos en las instalaciones y almacenados en un contenedor a prueba de fuego. Los respaldos completos de uso regular y calendarizado deben ser rotados a un complejo de almacenamiento fuera de las instalaciones para ser conservados por lo menos 30 días.

Las etiquetas de los medios de respaldo deben especificar la fecha de creación y la computadora de origen o computadoras; cuando sea apropiado, deben especificar la aplicación respaldada. Cuando los medios removibles de respaldo sean rotados en un complejo de almacenamiento fuera de las instalaciones, debe ser marcado con la fecha en que han ingresado al complejo y la fecha en la que deben ser retirados.

3.8. Requerimientos de Restauración.

El Instituto FONACOT es responsable de las actividades de restauración.

3.8.1. Procedimientos de Restauración.

Si se llegara a dañar o perder la información de los activos críticos determinados por la SGTIC durante las operaciones normales, la Subdirección de Soporte y Operación de Sistemas debe intentar restaurar la información usando el respaldo más reciente, el medio apropiado debe ser obtenido del almacenamiento fuera de las instalaciones y la información restaurada.

En una situación donde una copia antigua de un archivo es usada para restauración, se debe realizar lo siguiente:

- El personal que custodia los activos debe ser informado del problema y la fecha del archivo usado para la restauración.
- Se deben activar los procedimientos para restaurar los contenidos del archivo perdido por la actualización de la versión antigua de la información.
- En la restauración de un servidor en entorno virtual, se debe realizar la restauración de la información en un ambiente no productivo y con un servidor nuevo, incluyendo nuevos volúmenes de almacenamiento.

3.8.2. Recuperación de Medios y su Devolución al Lugar de Almacenamiento Fuera de las Instalaciones.

Se debe mantener registros de la extracción de medios de respaldo, así como de su devolución al complejo de almacenamiento fuera de las instalaciones. Los medios extraídos del almacenamiento deben ser devueltos tan pronto como la restauración sea completada.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.8.3. Restauración de un Disco Duro.

Si el disco duro de una laptop o servidor falla, se debe formatear un disco duro nuevo y se debe restaurar el contenido del disco perdido al disco nuevo. Los procedimientos operacionales estándar deben indicar la reconstitución de los discos duros, señalando en forma específica los drivers que contienen sistemas operativos y/o sistemas de bases de datos correlativos.

3.8.4. Reconstitución de Sistemas.

La reconstitución de sistemas que se han perdido debido a un evento catastrófico se debe considerar en los planes del PCN y DRP.

Cualquier procedimiento asociado con un plan debe indicar la protección continua de los medios de respaldo. Si se requiere un software o hardware para soportar el proceso de los medios de respaldo, se debe identificar la manera de señalar estos requerimientos antes de que el plan sea publicado.

3.8.5. Valuación de los Procedimientos de Restauración.

Los procedimientos de restauración deben ser revisados anualmente para asegurar que son efectivos y pueden ser completados en un período de tiempo apropiado con base en los requerimientos de disponibilidad del sistema y aplicación.

La revisión debe verificar que el proceso de restauración trabaja correctamente y la información es extraíble.

Los resultados de las pruebas deben ser reportados. Se debe discutir cualquier detalle identificado en las revisiones e identificar las posibles soluciones para resolverlo.

4. REGISTRO Y MONITOREO.

4.1. Registro de Eventos.

El área de Soporte y Operación de Sistemas debe realizar revisiones diarias y rutinarias de los registros de auditoría para detectar actividades maliciosas potenciales, estas revisiones deben documentarse. La revisión puede consistir en reportes formateados previa y automáticamente por alguna solución/herramienta o se puede realizar de manera manual.

Los documentos generados por el proceso de monitoreo de los sistemas deben clasificarse como confidencial, por lo que deben protegerse apropiadamente contra la modificación y el acceso no autorizado. Adicionalmente, los documentos generados por el proceso de monitoreo de sistemas deben mantenerse por un período de tiempo previamente definido por la SSOS, a fin de contar con esta información en caso de requerirse.

El registro de eventos debe contener al menos los siguientes elementos:

- ID.
- Inicio y cierre de sesión (Fecha, hora).
- Registro de los intentos de acceso rechazado por el sistema.
- Cambios en la configuración del sistema.
- Registro de actividades realizadas.

De existir alguna excepción debido a que el sistema y/o aplicación no permita alguno de estos elementos, se debe especificar en el registro como No aplicable y se debe incluir en una nota.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

4.2. Protección de la Información del Registro.

Los mecanismos para detectar y registrar los sucesos importantes relacionados con la seguridad de los equipos críticos del Instituto FONACOT deben ser resistentes a ataques y fraudes. Debe haber la protección adecuada para prevenir intentos de desactivar, modificar o borrar el software de registro y/o los registros.

Las fallas detectadas e incidentes de seguridad deben reportarse a las áreas apropiadas e involucradas, además de tomar la acción correctiva que corresponda.

Todos los sistemas del Instituto FONACOT que se encuentran en el ambiente de producción deben incluir bitácoras que registren al menos los siguientes datos:

- Cuenta y actividad de la sesión.
- Cambios a los archivos de sistema de las aplicaciones.
- El uso de comandos privilegiados (sudo).

Registros del administrador y operador.

El RSI debe revisar mensualmente las actividades registradas de los operadores y los administradores de los sistemas críticos, estos registros deben ser clasificados como confidenciales y se deben proteger del acceso no autorizado.

4.3. Sincronización del Reloj.

Los administradores de los sistemas operativos y aplicaciones deben asegurar que los relojes de estos se encuentren sincronizados de acuerdo con una misma fuente.

La configuración correcta del reloj de la computadora tiene como finalidad asegurar la precisión de los registros de seguridad y de la supervisión. Los registros de seguridad inadecuados pueden obstruir en revisiones o investigaciones, causando el daño en la credibilidad de dicha evidencia.

Siempre que sea posible, se deben sincronizar los relojes en forma automática con un reloj de tiempo real. Cuando no sea posible, los relojes deben ser sincronizados semanalmente en forma manual.

4.4. Gestión de Vulnerabilidades Técnicas.

El RSI debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados dentro del Instituto FONACOT, así como evaluar su grado de exposición a las mismas.

El RSI debe identificar los riesgos asociados a las vulnerabilidades y adoptar las medidas adecuadas y oportunas en respuesta a lo anterior.

4.5. Restricción en la Instalación de Software.

Las limitaciones y restricciones del uso del software son incluidas en los acuerdos de licencia que acompaña a cada paquete de software.

Está prohibido que el personal laboral y proveedores del Instituto FONACOT instalen software en los activos sin una aprobación por parte del RSI y de la SGTIC.

4.6. Controles de Auditoría a los Sistemas de Información.

El RSI debe planificar y acordar los requisitos y las actividades de auditoría interna que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Para esto se debe generar un reporte de auditoría que contenga:

- Número de recomendaciones.
- Descripción de la recomendación.
- Activo(s) relacionado en la recomendación.

Por último, se debe generar un plan que atenderá a cada recomendación y que debe describir:

- Número de recomendación.
- Descripción de la recomendación.
- Causa que provocó dicha recomendación.
- Área responsable.
- Actividades que dan cumplimiento.
- Tiempo de cumplimiento.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

8. POLÍTICA DE PROTECCIÓN CONTRA CIBERAMENAZAS.

1. INTRODUCCIÓN.

Las ciberamenazas cambian y evolucionan prácticamente al mismo tiempo que lo hace la propia tecnología, con este enfoque el Instituto FONACOT debe contar con soluciones tecnológicas que no solo se limiten a proteger ante una amenaza, sino que sean capaces de adelantarse a ella de manera inteligente.

2. PROTECCIÓN CONTRA CIBERAMENAZAS.

2.1. Responsabilidad del Instituto FONACOT.

El Instituto FONACOT debe implementar soluciones tecnológicas que brinden protección contra ciberamenazas considerando las denominadas amenaza avanzada persistente (APT), esta protección se debe realizar a través del análisis, monitoreo, anticipación y solución de aquellas amenazas que ponen en riesgo la red interna y los dispositivos endpoint.

3. INTELIGENCIA DE AMENAZAS.

La inteligencia de amenazas debe proporcionar al Instituto FONACOT el conocimiento del entorno de amenazas para que pueda tomar acciones de mitigación apropiadas.

La información sobre las amenazas existentes o emergentes se recoge y analiza para:

- a) Facilitar acciones informadas para evitar que las amenazas causen daño al Instituto FONACOT.
- b) Reducir el impacto de dichas amenazas.

La inteligencia sobre amenazas debe dividirse en tres niveles:

- a) Inteligencia sobre amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de las amenazas (por ejemplo, tipos de atacantes o tipos de ataques).
- b) Inteligencia sobre amenazas tácticas: información sobre las metodologías, herramientas y tecnologías de los atacantes.
- c) Inteligencia sobre amenazas operativas: detalles sobre ataques específicos, incluyendo indicadores técnicos.

La información sobre amenazas debe ser:

- a) Relacionada con la protección del Instituto FONACOT.
- b) Precisa y detallada, de manera que facilite la comprensión y panorama de las amenazas.
- c) Proporcione el conocimiento de la situación añadiendo contexto a la información en función del momento en que se producen los acontecimientos, el lugar donde se producen y las experiencias anteriores.
- d) Puntual para que permita actuar de forma eficaz.

Las actividades de inteligencia sobre amenazas deben incluir:

- a) Los objetivos de inteligencia sobre amenazas.
- b) Identificar, examinar y seleccionar las fuentes de información internas y externas que sean necesarias y adecuadas para proporcionar la información requerida para la producción de inteligencia sobre amenazas.
- c) Recoger información de las fuentes seleccionadas, que pueden ser internas y externas.
- d) Procesar la información recogida para prepararla para el análisis.
- e) Analizar la información para entender cómo se relaciona y el sentido que tiene para el Instituto FONACOT.
- f) Comunicar y compartir con las personas pertinentes.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

9. POLÍTICA DE CUMPLIMIENTO.

1. INTRODUCCIÓN.

El Instituto FONACOT debe evaluar los requerimientos legales y regulatorios aplicables a su entorno operacional y de negocio, y debe ejecutar procedimientos para mantener y monitorear el cumplimiento con dichos requerimientos.

El Instituto FONACOT está obligado a asegurar que tiene copias legales de software comercial y que cumple con cualquier restricción asociada con las licencias de este. Las copias ilegales de software son vistas como una violación y puede provocar en una acción disciplinaria conforme al Código de Ética de la Administración Pública Federal y al Código de Conducta del Instituto FONACOT.

Los encargados del software deben establecer contratos y condiciones generales de compra cuando sea posible. Bajo requerimiento de la Dirección de Recursos Materiales y Servicios Generales pueden dar soporte y proporcionar una guía en la fase de creación de contratos.

2. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES.

2.1. Identificación de la Legislación Aplicable y Requisitos Contractuales.

Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque del Instituto FONACOT para cumplir con los requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados para cada sistema de información.

En el Instituto FONACOT se refiere la documentación a través del Manual de Organización General en la sección IV. Marco Jurídico-Administrativo, documento que se encuentra en la intranet del Instituto FONACOT (<http://intranet/Paginas/default.aspx>) sección normateca, tipo de documento Manual.

2.2. Derechos de Propiedad Intelectual.

Los DPI incluyen licencias de código fuente del software, documentos de derechos de autor, derechos de diseño, marcas y patentes, que puedan pertenecer al Instituto FONACOT.

El Instituto FONACOT debe considerar las siguientes directrices para proteger cualquier material que pueda ser considerado propiedad intelectual.

- Uso legal del software y la información de los productos.
- La SGTIC adquirirá licencias de software a través de fuentes conocidas y de buena reputación, para asegurar que no se violen los derechos del autor.

2.3. Protección de Registros de la Organización.

Se deben seguir los principios para la conservación de registros organizacionales (registros importantes dentro del Instituto FONACOT que deben ser protegidos de pérdida, destrucción y falsificación). Los archivos deben asignarse de manera confidencial, íntegra y disponible con base en los estatutos, regulaciones u otros requerimientos para el archivo de registros.

Los registros deben ser clasificados en tipos de registro (ej.: contable, financiero o base de datos), con los requerimientos de retención y almacenamiento identificados para cada tipo. Los registros almacenados de manera encriptada requieren ser archivados con sus claves y necesitan estar disponibles en el sistema de cifrado.

Los registros almacenados de manera electrónica deben ser almacenados en medios con una vida de por lo menos el doble del período de retención.

Los procedimientos deben centrarse en la disponibilidad continua de la tecnología necesaria para el acceso a los registros a lo largo del período de retención. Los sistemas de almacenamiento de datos se deben seleccionar mediante requerimientos que incluyan las reglas de evidencia establecidas, ej.: los registros se pueden

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

recuperar en una forma calendarizada aceptable. El sistema de almacenamiento de datos debe permitir la identificación de registros, así como el vencimiento de su período de retención.

La persona que es el custodio de los activos de los archivos de registro debe determinar la disposición apropiada de los registros cuando el período de retención haya terminado.

2.4. Protección y Privacidad de la Información de Identificación Personal.

En cumplimiento con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Instituto FONACOT debe contar al menos con los siguientes documentos vigentes:

- Aviso de Privacidad.
- Procedimiento y solicitud para atender derechos ARCO (acceso, rectificación, cancelación y oposición).
- Inventario de datos personales.
- Responsables.
- Medidas compensatorias técnicas, físicas y administrativas.

2.5. Regulación de Controles Criptográficos.

El Instituto FONACOT debe apegarse a la Política de Criptografía.

3. GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADA Y OPERADA.

3.1. Revisión Independiente de la Seguridad de la Información.

El Instituto FONACOT a través del RSI debe revisar y actualizar las políticas, procedimientos, controles y estándares de seguridad de la información, con base en un plan de revisión predefinido, requiriendo al menos una revisión anual.

Las políticas de seguridad informática, procedimientos y/o controles que representen tecnologías emergentes o de rápido cambio se deben evaluar con mayor frecuencia. Se debe evaluar la continuidad en relevancia y efectividad de cada política, para proteger los activos informáticos del Instituto FONACOT durante la revisión de cada política de seguridad, se debe considerar la evaluación de los siguientes factores:

- El efecto de los cambios a la infraestructura y ambiente técnico.
- Identificación de nuevas vulnerabilidades que puedan colocar en riesgo de seguridad al Instituto FONACOT.
- Factores técnicos o de negocio que afecten o cambien el resultado de valuaciones de riesgo previas.
- El impacto y costo de los controles de seguridad sobre la eficiencia del negocio.
- Iniciativas o directrices de negocio, nuevas o emergentes.
- Iniciativas o directrices tecnológicas, nuevas o emergentes.

3.2. Cumplimiento con Políticas y Normas de Seguridad de la Información.

La implementación de políticas debe ser revisada de forma anual por el RSI para asegurar que las prácticas organizacionales cumplan con lo estipulado dentro del MGSI del Instituto FONACOT.

Las revisiones deben incluir una verificación de que se cumplen técnicamente, llevada a cabo y supervisada por personal técnicamente competente; en el momento adecuado, para la configuración de componentes, el escaneo de evaluación de vulnerabilidades, así como pruebas de penetración, pueden ser adecuadas. Esta revisión se denomina auditoría interna del MGSI, liderada por las áreas de Dirección de Auditoría Interna y la Subdirección General de Contraloría, Planeación y Evaluación.

3.3. Comprobación del Cumplimiento Técnico.

Se debe llevar a cabo revisiones trimestrales para verificar el cumplimiento del estándar técnico de controles mínimos de seguridad de la información establecidos por la CEDN.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

10. POLÍTICA DE SEGURIDAD EN LOS RECURSOS HUMANOS.

1. INTRODUCCIÓN.

Esta política de seguridad de la información tiene el objetivo de proporcionar los requerimientos mínimos que debe seguir el personal laboral del Instituto FONACOT y externos que tienen acceso garantizado a los activos informáticos del Instituto FONACOT.

Los elementos principales de protección requeridos por esta política son:

- Una selección apropiada del personal del Instituto FONACOT que debe ser conducida hasta garantizar el acceso a los activos de información.
- Asegurar que los convenios de secrecía, confidencialidad, reserva, no revelación, uso y/o divulgación de información esté firmado por cada persona antes de autorizar el acceso a los activos del Instituto.

El Instituto FONACOT adicionalmente cuenta con el Manual de Políticas y Procedimientos de la Dirección de Recursos Humanos.

2. SEGURIDAD EN RECURSOS HUMANOS.

Las medidas de la seguridad del personal laboral son implementadas para minimizar el riesgo que puede estar asociado o no intencionalmente, con una fuerza de trabajo diversa y amplia. Las medidas incluyen los procedimientos para monitorear a los aspirantes de empleo para identificar “personas problemas” antes de que se conviertan en personal laboral, así como para asegurar su competencia.

2.1 Previo al Empleo.

La Dirección de Recursos Humanos debe asegurarse que se lleva a cabo la evaluación previa a la contratación del personal de ingreso o candidatos/postulantes a ocupar una vacante del Instituto FONACOT y a terceros involucrados, antes de que asuman cualquier responsabilidad.

El Instituto FONACOT realiza la evaluación y selección de candidatos de confianza y sindicalizados dentro del rango del nivel operativo hasta el nivel dirección, por medio de la revisión de los siguientes puntos:

- Cubrir el Perfil de Puesto.
- Entrevista por Competencias.
- Entrevista Técnica por la persona de nivel superior inmediato.
- Evaluación Psicométrica.
- Calificación de entrevista técnica.
- Encuesta Socioeconómica.

La evaluación debe ser realizada por la Dirección de Recursos Humanos. La evaluación mínima debe comprender en cumplimiento con las leyes y regulaciones cuando menos lo siguiente:

- Identificación oficial vigente.
- Revisión del Currículum Vitae.
- Revisión del último comprobante de estudios.
- Revisión de referencias.
- Cartas de recomendación (*Sólo para el personal laboral operativo*).
- Estudio Socioeconómico.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.1.1 Políticas e Investigación del Personal.

Todas las personas candidatas/postulantes a ocupar una vacante (ya sea personal laboral o externo) están sujetos a cumplir con los niveles básicos de investigación por parte del Instituto FONACOT, previamente a comenzar a laborar en esta y/o antes de que el personal laboral sea promovido y se le asigne un rol que incremente sus accesos a información o activos confidenciales o críticos.

El proceso de investigación es aplicado al personal laboral de nuevo ingreso dentro del rango del nivel operativo hasta el nivel dirección, esta actividad es realizada por un tercero y validada por la Dirección de Recursos Humanos del Instituto FONACOT; tiene como objetivo verificar la documentación del aspirante y evaluar su integridad. Dicho proceso se aplica cuando una persona empieza a laborar y es el siguiente:

- Verificar dos referencias de compañías en las que haya laborado con procedimientos que permitan validar la información.
- La Dirección de Recursos Humanos y el proveedor contratado para realizar los Estudios Socioeconómicos son los únicos encargados de realizar la revisión de las referencias.
- Confirmación de los documentos solicitados (original o copias dependiendo del documento). Es necesaria la entrega de los documentos solicitados. Referenciar el documento que hace mención del proceso que se sigue de acuerdo con el comentario.

El Instituto FONACOT debe mantener los registros del personal laboral y proveedores que han dejado de laborar o prestar su servicio en el Instituto FONACOT de manera involuntaria, los cuales no se recontractarán sin una aprobación de la Subdirección General de Administración, así como de la Unidad Administrativa que esté solicitando su reingreso.

2.1.2 Convenio de Secrecía, Confidencialidad, Reserva, No Revelación, Uso y/o Divulgación de Información.

Todo el personal laboral de nuevo ingreso debe firmar el formato de Convenio de secrecía, confidencialidad, reserva, no revelación, uso y/o divulgación de información antes de permitirles el acceso a los sistemas de información del Instituto FONACOT.

3 SEGURIDAD DURANTE EL EMPLEO.

3.1 Responsabilidad de la Dirección.

La Dirección General, a través de la Dirección de Recursos Humanos, se asegura que todo el personal del Instituto FONACOT es consciente de las amenazas que giran en torno a la seguridad de la información, así como sus responsabilidades, y están provistos con lo necesario para dar cumplimiento con las políticas de seguridad en sus labores, y así reducir el riesgo de errores humanos.

La Dirección de Recursos Humanos debe promover la capacitación del personal laboral con los elementos necesarios para asegurar que entienden totalmente las políticas, estándares y procedimientos de seguridad durante su período de empleo en el Instituto FONACOT.

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

Los registros de la capacitación provista por el Instituto FONACOT o pruebas de capacitación del personal laboral son necesarios para calificar las nuevas posiciones. Estos deben ser archivados durante el período de empleo.

3.2.1 Capacitación en Concientización de Seguridad de la Información.

Todo el personal laboral involucrado en el alcance del MGSI debe recibir concientización de seguridad de la información, cuando se unen al Instituto FONACOT, participando en el curso de Inducción *E-learning*, en el cual se incluye un módulo específico para la seguridad de la información y un reforzamiento de manera anual. La capacitación recibida debe ser documentada en el expediente de cada persona y el registro debe ser retenido durante el período de empleo.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

El entrenamiento anual debe abordar todos los aspectos y responsabilidades del personal laboral definidos en las políticas de seguridad de la información del Instituto FONACOT.

3.2.2 Recordatorios Trimestrales.

Se debe transmitir información, boletín, correo electrónico y/o imagen de las responsabilidades de seguridad del personal laboral bajo las políticas de seguridad de la información del Instituto FONACOT de manera trimestral.

4 TERMINACIÓN Y CAMBIO DE EMPLEO.

Con el propósito de reducir el riesgo que se tiene respecto a la confidencialidad, integridad y disponibilidad de los activos de información y activos relacionados del Instituto FONACOT ante el despido o finalización voluntaria de relaciones contractuales de cualquier elemento del personal laboral o proveedor, el Instituto FONACOT debe establecer las medidas de control necesarias.

4.1 Despidos y Finalizaciones de Relaciones Contractuales.

Al personal laboral que deje de prestar sus servicios en el Instituto FONACOT se le debe recordar su obligación de mantener la confidencialidad de la información a la que tuvieron acceso durante el tiempo que laboraron en el Instituto FONACOT.

Cuando existe una finalización de relaciones contractuales, el personal laboral y proveedores deben regresar a la persona que ocupe el nivel jerárquico superior inmediato todos los activos y copias de la información del Instituto FONACOT, recibidas y/o creadas durante la vigencia de su contrato. La entrega debe hacerse al personal laboral responsable de los activos antes de abandonar las instalaciones del Instituto FONACOT.

La lista de verificación de salida debe ser usada de manera individual, con el fin de asegurar que se ejecuten de manera completa las actividades requeridas para su finalización de relaciones contractuales. Esta lista debe ser revisada por la Dirección de Recursos Humanos antes de que el personal laboral relacionado abandone las instalaciones del Instituto FONACOT.

En caso de finalización de relaciones contractuales, la Dirección de Recursos Humanos debe realizar las notificaciones y acciones apropiadas de manera inmediata o por adelantado, para asegurar que tanto el acceso lógico como físico se ha cerrado y que todos los activos del Instituto FONACOT sean devueltos antes de que el personal laboral involucrado abandone las instalaciones.

Esto incluye, como mínimo, notificar a las áreas de SGCyR, SGTIC, Abogado(a) General y DRMySG.

4.2 Recuperación de Activos de Información y Equipo.

Todos los activos de información o activos relacionados asignados al personal laboral despedido o que haya finalizado voluntariamente su relación contractual con el Instituto FONACOT (por ejemplo: consultores) deben recuperarse en forma inmediata y previamente a que la persona o personas abandonen las instalaciones.

4.3 Revocación de Derechos de Acceso por Despido o Finalización Voluntaria de Relaciones Contractuales del Personal Laboral y Proveedores.

Todos los accesos a sistemas deben revocarse en la fecha en que se emitan las órdenes de despido o finalización voluntaria de relaciones contractuales con el Instituto FONACOT.

El acceso físico a las instalaciones del Instituto FONACOT debe revocarse y restringirse en forma inmediata a la generación de la orden de despido o finalización voluntaria de relaciones contractuales.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

11. POLÍTICA DE PANTALLA Y ESCRITORIO SEGURO.

1. INTRODUCCIÓN.

Esta política tiene como objetivo definir y establecer las medidas preventivas en materia de protección de la información con la que el personal y/o terceros desarrollan, procesan y almacenan información en la infraestructura del Instituto FONACOT.

Esta política aborda los siguientes principios de protección:

- Las instalaciones del Instituto FONACOT que almacenan la información del Instituto FONACOT deben estar físicamente protegidas de accesos no autorizados, daños e interferencia y deben estar protegidos por un perímetro definido, con controles de entrada y barreras de seguridad apropiados.
- La clasificación de la información, las instalaciones se ubican dentro de un perímetro de seguridad definido.
- La clasificación de las computadoras y cualquier otro equipo de procesamiento de datos se encuentran ubicados en un lugar seguro.
- El equipo debe estar protegido contra amenazas a la seguridad y riesgos ambientales.

2. PANTALLA Y ESCRITORIO LIMPIO.

El personal laboral debe limpiar sus escritorios y áreas de trabajo antes de retirarse y asegurarse de que toda la información confidencial queda correctamente protegida, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de información fuera de las horas normales de trabajo, como se describe a continuación:

- Los medios de almacenamiento de información impresa y electrónica clasificada como confidencial, debe guardarse en gabinetes bajo llave cuando no hay nadie en la oficina.
- El personal laboral debe revisar que no quede ningún documento en las impresoras y fotocopiadoras antes de abandonar la oficina.
- Las áreas de entrada y salida de correo o correspondencia, así como las impresoras, deben estar adecuadamente protegidas.
- Los cajones de los escritorios y los gabinetes deben cerrarse bajo llave cuando no haya nadie en la oficina y las llaves deben guardarse en un lugar seguro.
- A las computadoras que se encuentran en el dominio fonacot.gob.mx se les aplica una política que bloquea la sesión y activa el protector de pantalla después de 300 segundos (5 minutos) de inactividad. Para desbloquear y tener acceso a los recursos de red, es necesario volver a ingresar la contraseña de inicio de sesión.

2.1. Equipo de Cómputo Desatendido.

- El personal es responsable de terminar la conexión después de terminar sus labores.
- El personal es responsable de bloquear su computadora antes de levantarse de su lugar y dejarla desatendida, en todo caso debe proteger la información de accesos no autorizados.
- Los dispositivos o medios que almacenan información confidencial deben estar protegidos física y lógicamente de accesos no autorizados.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

12. POLÍTICA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

Este documento se enfoca en los roles relacionados con la seguridad de la información y sus responsabilidades, de una serie de políticas y estándares de la seguridad de la información en las operaciones del Instituto FONACOT.

2. ROLES DE SEGURIDAD EN EL INSTITUTO FONACOT.

2.1. Responsable de la Seguridad de la Información en el Instituto FONACOT.

- Integrar el Equipo de Respuesta a Incidentes de Seguridad en TIC.
- Dar seguimiento a la conformación del MGSI, así como a su implementación y al cumplimiento de los controles mínimos de seguridad.
- Presentar a sus superiores jerárquicos, incluida la persona titular del Instituto FONACOT, un informe anual sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución.
- Dar aviso inmediato al CERT-MX y/o policía cibernética sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.
- Implementar un programa de evaluaciones, que contemple verificar el desempeño de los controles de seguridad y determinar acciones de mejora.
- Hacer del conocimiento del OICE en el Instituto FONACOT y/o de las autoridades competentes, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia.
- Mantener un proceso de Mejora Continua del MGSI para cumplir con las disposiciones aplicables.
- Realizar campañas de concientización sobre seguridad de la información, así como, capacitaciones especializadas para los equipos de respuesta del Instituto FONACOT.
- Implementar herramientas de monitoreo y detección de incidentes.

El RSI crea grupos de trabajo para la definición, implementación y evaluación del MGSI, los cuales se conforman de la siguiente manera.

2.2. Equipo de Respuesta a Incidentes de Seguridad en TIC.

- Identificación y actualización de activos esenciales de información.
- Elaboración y actualización del PCN de TIC.
- Realizar la gestión y monitoreo proactivo para la gestión de incidentes.
- Contener y mitigar la amenaza con recursos del Instituto FONACOT o externos.
- Recuperar los servicios esenciales.
- Identificación de indicadores de compromiso.
- Desarrollo de las actividades post-incidente que incluye entre ellas la presentación de la denuncia ante el Ministerio Público, con ayuda de las áreas pertinentes dentro del Instituto FONACOT.
- Intercambiar activamente información con el CERT-MX y/o policía cibernética.
- Establecer el mecanismo de registro de los incidentes de seguridad de la información.
- Reportar al RSI, los incidentes de seguridad de la información que se presenten.
- Integrar los datos del incidente y su solución a los repositorios del Instituto FONACOT.
- Realizar las acciones de preparación, detección, respuesta y recuperación de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3. ROLES INDIVIDUALES DE SEGURIDAD DE LA INFORMACIÓN.

3.1. Personal que Custodia los **Activos**.

El personal que custodia los activos, son responsables de las siguientes acciones con respecto a la seguridad informática:

- Responsable de valorar riesgos asociados con el activo.
- Responsable de proteger los activos informáticos asignados.
- Asignar clasificaciones de confidencialidad, integridad y disponibilidad a los activos informáticos asignados.
- Aprobar o rechazar solicitudes de acceso físico o lógico asociados con activos asignados, incluyendo el acceso a archivos/directorios, conexiones de red y préstamos de activos físicos.
- Investigar los incidentes de seguridad que involucran los activos asignados.
- Es responsable de responder a las actividades asociadas con una cuenta asignada, así como del equipo y los dispositivos removibles asignados.
- Proteger la confidencialidad de su contraseña.
- Reportar a la Mesa de Servicio los incidentes de seguridad conocidos o que son motivo de sospecha.

4. CONTACTO CON LAS AUTORIDADES.

El Instituto FONACOT debe mantener todos los contactos apropiados con las autoridades relevantes; requeridas para apoyar la gestión de los diferentes incidentes de seguridad de la información o la continuidad de negocio y la contingencia.

El Instituto FONACOT debe tener contacto con otras autoridades, protección civil, seguridad y salud, como pueden ser los bomberos, los proveedores de telecomunicaciones, los proveedores de luz, agua, entre otros. Estos datos deben mantenerse actualizados permanentemente.

5. CONTACTO CON EL GRUPO DE ESPECIAL INTERÉS.

El Instituto FONACOT debe mantener contacto con todos los grupos de interés en los diferentes foros de seguridad y asociaciones profesionales.

Los beneficios que ofrece estar en contacto con los foros de seguridad y las asociaciones profesionales son:

- La mejora del conocimiento sobre las prácticas y encontrarse actualizado con información relevante de seguridad.
- Hay que asegurar que el entendimiento del ambiente de Seguridad de la Información es actual y completo.
- Recibir todas las alertas de detección temprana, advertencias y parches que sirve para solventar ataques y vulnerabilidades.
- Conseguir acceder a consejos especializados de Seguridad de la Información.
- Compartir información sobre las nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Proveer puntos de enlaces convenientes cuando se consigue obtener información de incidentes de seguridad.

Es necesario llegar a acuerdos para poder compartir la información, esto ayuda a mejorar la cooperación y la coordinación entre los diferentes temas de seguridad. Los acuerdos tienen que identificar todos los requerimientos para proteger la información sensible.

6. SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN DE PROYECTOS.

Todos los proyectos del Instituto FONACOT deben contener el rubro de seguridad de la información y forma en que se dará atención a través de los lineamientos designados dentro del acuerdo por el que se emiten las

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

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, publicado en el D.O.F. el 06 de septiembre de 2021.

7. DISPOSITIVOS MÓVILES.

Cualquier persona que tenga asignado un equipo de comunicación a los que determine tengan la necesidad de ocupar esta herramienta y será para el uso exclusivo de la persona asignada. Las únicas excepciones están determinadas por la Unidad Administrativa correspondiente.

- Se asignará un equipo según las necesidades del solicitante. Una vez asignado será para el uso exclusivo de la persona asignada. Las únicas excepciones están determinadas por la Dirección de la Unidad Administrativa correspondiente.
- El personal laboral tienen un perfil limitado y utilizan sus equipos únicamente para efectos de trabajo.
- Queda restringido el acceso a la red del Instituto a través de dispositivos móviles personales, excepto los asignados y proporcionados por el Instituto FONACOT.
- Cuando un cliente o proveedor requiera hacer uso de algún dispositivo móvil dentro de las áreas operativas, debe solicitar la autorización al responsable del área.
- Queda prohibido tomar fotografías dentro de las instalaciones del Instituto FONACOT, excepto para cuestiones laborales.

La asignación de equipos de comunicación debe apegarse con lo establecido en la Ley Federal de Austeridad Republicana, Artículo 16, Fracción VIII.

8. TELETRABAJO.

Cualquier persona que realice trabajo a distancia conectándose a la infraestructura del Instituto FONACOT y centro de datos, debe cumplir con los lineamientos que apliquen al tipo de dispositivo, establecidos en las políticas de dispositivo móvil, política de control de acceso, política de pantalla y escritorio limpio, así como las siguientes políticas:

- Llevar un registro de la persona, entorno y el equipo autorizado para realizar trabajo a distancia.
- Utilizar únicamente el equipo autorizado para el teletrabajo.
- Crear una cuenta al equipo específico para fines laborales (Si se utiliza un equipo personal).
- Activar mecanismos de control de acceso de esa cuenta y bloqueo del equipo.
- Toda la información creada desde un equipo propiedad del Instituto FONACOT, equipo personal, o a través del perfil asignado para fines laborales, será considerada como propiedad del Instituto FONACOT.
- Almacenar la información del Instituto FONACOT en el repositorio establecido.
- Permitir y autorizar la instalación o configuración de software establecido por el área, nombre del área de sistemas/ seguridad /TI o a fin, el cual permite proteger la información y el uso de esta.
- Desactivar las funciones de red como bluetooth, funciones de red que permitan compartir recursos o archivos y activarlas cuando se necesiten.
- Contar con un antivirus actualizado.
- Activar el protector de pantalla del equipo, tiempo para bloquear el equipo 5 minutos.
- Instalar y utilizar solo software conocido y confiable.
- Mantener el software actualizado.
- Mantener la configuración del software de acceso remoto establecida por el Instituto FONACOT.
- El acceso remoto a la red interna del Instituto FONACOT fuera del horario establecido se considera como un caso urgente y se requiere de una notificación y autorización escrita (correo, mensaje de texto) de la gerencia y dirección del área.
- Cambiar las contraseñas de sistemas, y aplicaciones conforme a los lineamientos establecidos por el Instituto FONACOT.

 <p>TRABAJO SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</p>	<p>MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT</p>	<p>Clave: MA26.01</p> <p>Vigencia: Julio, 2024</p>	
---	--	--	---

- No instalar software que permita la explotación de riesgos que comprometan la seguridad de la información o el incumplimiento de leyes o regulaciones.

Adicionalmente, el teletrabajo debe apegarse con lo establecido en el capítulo XII BIS Teletrabajo de la Ley Federal de Trabajo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

13. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

Esta política para la seguridad de la información tiene como propósito proporcionar los requerimientos para reportar y responder a incidentes de seguridad.

La aplicación de esta política es permitir respuestas rápidas, apropiadas y efectivas a incidentes de seguridad con el fin de minimizar la duración y el alcance del incidente y los daños causados.

Esta política aborda los siguientes elementos de protección:

- Procedimiento de gestión de incidentes.
- Mantenimiento de una base de datos de incidentes de seguridad para permitir actividades de administración de riesgos, así como el cumplimiento de requerimientos reguladores para el reporte de incidentes.
- Asignación de responsabilidades para el reporte y la respuesta de incidentes.

2. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS.

2.1. Responsabilidades y Procedimientos.

Responsabilidades para la notificación o tratamiento del incidente:

- Todo el personal debe reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.
- La persona que es el custodio de los activos de información debe reportar al Instituto FONACOT los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- El Instituto FONACOT debe evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar a aquellos en los que considere pertinente.
- El Instituto FONACOT debe asignar personal calificado para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una evaluación exhaustiva y proporcionando las soluciones.
- El Instituto FONACOT debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dicha base de conocimiento.
- El RSI, en caso de incidente de seguridad de la información, debe notificar a la CEDN, a la Dirección de Contraloría Interna y SG TIC, en caso de eventos cibernéticos notificar a la policía cibernética.

El Instituto FONACOT debe desarrollar un Procedimiento de Incidentes que contenga cuando menos las siguientes actividades, así como de conformidad al Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos:

- Notificar un incidente.
- Registrar incidente.
- ¿Es un incidente de seguridad?
- Escalar o atender.
- Evaluar el incidente.
- Actividades necesarias para recopilar la evidencia.
- Escalar al grupo especialista o proveedor.
- Documentar la solución del incidente y notificar al personal involucrado.
- Cerrar el incidente.
- Registrar el aprendizaje.
- Revisar la solución.
- Elaborar el informe de incidentes.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.2. Notificación de los Eventos de Seguridad de la Información.

Todos los eventos de seguridad de la información se deben informar y reportar a través del procedimiento de incidentes de seguridad.

El personal laboral contratista y terceros deben estar al tanto del procedimiento de incidentes de seguridad para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos del Instituto FONACOT.

2.2.1. Mecanismos para Reportar Eventos de Seguridad de la Información.

El personal debe reportar cualquier incidente de seguridad a la Mesa de Servicio (*111).

El mecanismo de reporte debe estar monitoreado y los procedimientos deben garantizar una respuesta oportuna y eficaz.

2.2.2. Registro de los Reportes de Incidentes de la Seguridad.

Todos los reportes de posibles incidentes de seguridad se deben identificar y registrar de manera independiente. Los registros de incidentes deben conservarse durante un periodo no menor a tres años. Los registros de incidentes deben reportarse a la Dirección General.

2.2.3. Rastreo de los Reportes de Incidentes de la Seguridad.

Se debe permitir el continuo rastreo del estatus de la respuesta a un reporte de incidente de seguridad.

2.3. Notificación de Puntos Débiles de la Seguridad.

En caso de que se identifiquen áreas de oportunidad que se desprendan de un incidente de seguridad, se debe notificar y registrar a través del procedimiento de incidentes de seguridad, con el objetivo de prevenir riesgos a los activos de información del Instituto FONACOT.

2.4. Evaluación y Decisión Sobre los Eventos de Seguridad de la Información.

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base al análisis de riesgos y la clasificación de activos en el Instituto FONACOT.

La severidad del incidente puede ser:

- Alto Impacto: El incidente de seguridad afecta a activos de información que afecten la reputación y aspectos legales del Instituto FONACOT. Estos incidentes deben tener respuesta inmediata.
- Medio Impacto: El incidente de seguridad afecta a activos de información que influyen directamente a los objetivos de un proceso determinado.
- Bajo Impacto: El incidente de seguridad afecta a activos de información que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

2.5. Respuesta a Incidentes de Seguridad de la Información.

La respuesta a un posible incidente de seguridad debe guiarse por el principio de minimizar de manera proactiva el daño a los activos, reputación y los socios del Instituto FONACOT.

La recepción de un reporte de incidente se debe iniciar con una investigación basada en la categoría del posible incidente de seguridad. El procedimiento de gestión de incidentes debe contener los mecanismos de respuesta apropiada a los diferentes tipos de incidentes.

También se debe asignar responsabilidades de toma de decisiones en todo el proceso de respuesta.

Los incidentes de seguridad detectados deben incluir la respuesta detallando lo siguiente:

- Recopilación de evidencia tan pronto como sea posible después de la ocurrencia.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- El escalamiento del incidente, según sea necesario.
- Comunicación de los incidentes de seguridad de la información a personas internas y terceros.
- Garantizar que todas las actividades de respuesta involucradas se registran adecuadamente.
- Cerrar formal el incidente cuando se haya tratado con éxito y realizar el registro.

2.5.1. Respuesta a Incidentes que Involucran al Personal Laboral del Instituto FONACOT.

Cuando el personal del Instituto FONACOT esté involucrado en incidentes de seguridad de la información que resulten en alguna violación al proceso disciplinario del Instituto FONACOT, se procede en consecuencia, determinando el cauce que se le debe dar (administrativo, laboral o judicial) conforme al Código de Ética de la Administración Pública Federal, y al Código de Conducta del Instituto FONACOT.

2.5.2. Respuesta a Incidentes que Involucran la Disponibilidad de Experiencia Especializada.

Los requerimientos de la experiencia especializada para responder a un tipo particular de incidente se deben identificar en los procedimientos de respuesta a incidentes.

La seguridad de la información debe asegurar la disponibilidad de personas con la experiencia requerida sobre una base apropiada (ej.: a solicitud o demanda).

Se debe identificar las áreas que no puedan ser apoyadas internamente y los procedimientos de respuesta a incidentes deben indicar el apoyo para dichas áreas.

Se deben establecer acuerdos de no divulgación y de confidencialidad antes de involucrar a una persona ajena al Instituto FONACOT en respuesta a un incidente de seguridad.

2.5.3. Respuesta a Incidentes que Involucran el Cumplimiento de la Ley.

Los criterios para incluir organismos legales en la investigación o respuesta de incidentes se deben abordar en los procedimientos de respuesta a incidentes apropiados. Si es necesario, se deben proporcionar los criterios para determinar la oportunidad de contactar estos organismos.

2.5.4. Respuesta a Incidentes que Requieren el Apoyo del Distribuidor.

Es probable que la investigación o la respuesta a incidentes de seguridad requieran el apoyo de un distribuidor de hardware o software. Se deben establecer acuerdos de confidencialidad antes de dar a conocer a cualquier distribuidor información referente a un incidente de seguridad. Los Procedimientos de Respuesta a Incidentes deben incluir este requisito.

2.6. Comunicación con Terceros en Cuanto a un Incidente de Seguridad.

El RSI debe notificar al CERT-MX y/o policía cibernética.

Se debe prohibir a todo el personal laboral, contratistas o socios la divulgación de cualquier información a cualquier persona o entidad externa en cuanto a un posible incidente de seguridad.

2.7. Comunicación Interna en Cuanto a un Incidente de Seguridad.

El RSI debe contar con una base de datos con información relacionada con los eventos históricos relacionados con los incidentes de seguridad, conforme a lo indicado por la CNBV.

2.8. Requerimientos Organizacionales para Reportar Incidentes.

2.8.1. Incidentes de Seguridad que Involucran Conexiones Externas.

Un incidente de seguridad que involucre la explotación de una o más vulnerabilidades asociadas con una conexión externa se debe reportar de inmediato al personal que custodia los activos de la conexión externa.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.8.2. Incidentes de Seguridad que Involucran a un tercero.

Los contratos con terceros deben incluir la cooperación con la investigación de incidentes de seguridad que involucran al Instituto FONACOT y a un tercero.

Un incidente de seguridad que involucra una falla por parte de un tercero debe reportarse al área correspondiente, para aplicar a este las penas convencionales o deductivas previstas en el contrato, o bien, integrar la información para dar inicio al procedimiento de rescisión administrativa del contrato.

2.8.3. Incidentes de Seguridad que Involucran a un Cliente del Instituto FONACOT.

Un incidente de seguridad que involucra a un cliente del Instituto FONACOT o información privada relacionada con un cliente debe reportarse de inmediato a la Subdirección General de Tecnologías de la Información y Comunicación.

2.8.4. Incidentes que Requieren la Activación de Planes de Contingencia o Recuperación de Desastres.

Es probable que la respuesta a un incidente de seguridad requiera la activación de uno o más planes de contingencia o recuperación de desastres.

2.8.5 Incidentes de Seguridad que Involucren Sitios Web Apócrifos.

El Instituto FONACOT debe validar que los sitios web sean válidos, identificando todos aquellos que no formen parte de sus soluciones y que sean identificados como apócrifos, en tal caso el RSI debe reportar de inmediato a la policía cibernética y a la SGTIC para las acciones que correspondan.

2.9. Aprendizaje de los incidentes de seguridad de la información.

El Instituto FONACOT debe asegurarse que los reportes cuenten con un apartado para describir los aprendizajes sobre los incidentes que ayudan para determinar mejoras en los procesos, tecnologías y capacidades de respuesta.

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de mejorar o adicionar controles para limitar la frecuencia, el daño y el costo de futuras ocurrencias.

2.10. Recopilación de Evidencias.

El Instituto FONACOT debe definir y aplicar procedimientos para identificación, recopilación, adquisición y preservación de la información que puede servir como evidencia.

Al menos se deben realizar las siguientes actividades:

- La cadena de custodia.
- La seguridad de las pruebas.
- La documentación.

El Instituto FONACOT debe resguardar los registros generados a través de la mesa de servicio y registro de tickets.

2.11. Monitoreo y Seguimiento a Incidentes de Seguridad.

Se debe dar monitoreo y seguimiento a cada incidente de seguridad reportado. Este informe debe ser presentado al RSI.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

14. POLÍTICA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO.

1 INTRODUCCIÓN.

Esta política tiene como objetivo proveer una manera consistente para desarrollar y mantener planes de continuidad del negocio y actividades relacionadas con recursos informáticos a lo largo del Instituto FONACOT.

Esta política se avoca principalmente a los siguientes elementos:

- Establecer recursos informáticos para desarrollar y mantener planes de continuidad de negocio.
- Definir roles organizacionales para actividades de administración de continuidad del negocio, y asignar responsabilidades relacionadas con esos roles.

2 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

El Instituto FONACOT debe asegurarse de integrar la continuidad de seguridad de la información dentro de los planes de contingencia establecidos.

2.1. Planificación de la Continuidad de la Seguridad de la Información.

El Instituto FONACOT debe planear las personas, lugares, procedimientos, herramientas de TI o cualquier otro equipo especializado requerido y/o existente para la continuidad de sus actividades críticas.

El DRP debe permitir la entrega de estos servicios esenciales de TI a una ubicación de negocio alterna del Instituto FONACOT y debe contener información de los contactos con autoridades locales y equipos de rescate y emergencia.

Los requisitos de seguridad de la información establecidos en la Política General de Seguridad de la Información deben mantenerse en la medida razonable, aún en situaciones adversas.

2.2. Implementar la Continuidad de la Seguridad de la Información.

El Instituto FONACOT debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para gestionar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.

El Instituto FONACOT debe asegurarse que:

- Se designa al personal laboral con la responsabilidad, autoridad y competencia necesario para gestionar un incidente y mantener la seguridad de la información en caso de una contingencia.
- Tener una estructura de gestión adecuada implementada para preparar, mitigar y responder ante un incidente.
- Tener los procedimientos de recuperación, respuesta y planes detallando como el Instituto FONACOT se encarga de un incidente y mantiene la seguridad de la información a un nivel predeterminado.

2.3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información.

El Instituto FONACOT debe verificar la continuidad de la seguridad de la información a través de:

- El ejercicio y prueba de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información.
- El ejercicio y prueba de conocimiento de la rutina para operar los procesos, los procedimientos y los controles de la continuidad de seguridad de la información.
- La revisión de la validez y eficacia de las medidas de continuidad de seguridad de la información.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.3.1. Mantenimiento de Planes de Continuidad de Negocio.

Todos los planes de continuidad de negocio deben ser actualizados al menos una vez al año. La información de los contactos es esencial y debe ser revisada y actualizada al menos dos veces al año.

2.3.2. Simulacros de los Planes de Continuidad de Negocio.

Los planes de continuidad de negocio deben tener simulacros al menos una vez por año para lograr una Mejora Continua. El DRP debe ser simulado al menos una vez al año y preferentemente después de cada implementación importante de sistemas.

2.3.3. Ejecución de los Planes de Continuidad de Negocio.

Cuando se detecta una contingencia, la persona que lo haga debe notificar al responsable del área, sistemas o subdirección de TI, el cual debe haber sido previsto con las instrucciones necesarias para activar la administración de crisis. Una vez que queda claro que las instalaciones no están disponibles para una operación normal, el PCN debe ser ejecutado. Cada PCN debe tener asociados procedimientos para alertar al personal laboral adecuado del Instituto FONACOT.

2.4. Responsabilidad de la Administración de la Continuidad de Negocio.

El Instituto FONACOT debe nombrar a un administrador de la continuidad del negocio, quien tendrá la responsabilidad de asegurar que el negocio esté consciente de las políticas o estándares relacionados con la continuidad de negocio.

El Instituto FONACOT será responsable de los contenidos y calidad de los planes y debe asegurar que las copias hayan sido distribuidas a los involucrados. Al menos una copia del plan debe ser almacenada en un lugar seguro fuera de las instalaciones normales.

2.5. Programa de Continuidad de Negocio.

El Instituto FONACOT debe establecer un programa de continuidad de negocio. El programa debe basarse en una valoración inicial de las pérdidas que tendría como consecuencia de una repentina e inesperada interrupción del negocio.

Los riesgos específicos relacionados con la ubicación de la entidad también deben ser tomados en cuenta. El PCN debe ser revisado y aprobado por la Contraloría Interna, áreas de negocio y el RSI.

2.6. Requerimientos para Reportar y Responder a Incidentes.

El PCN del Instituto FONACOT debe permitir la rápida reanudación de las actividades críticas para salvaguardar el negocio y la reputación del Instituto FONACOT. La pérdida de las instalaciones es tomada como el punto de arranque para la activación del PCN.

El plan debe estar basado en los resultados de una valoración de riesgos que identifiquen los riesgos más relevantes para el negocio o el medio ambiente en el cual opera.

3 REDUNDANCIAS.

Se debe garantizar la disponibilidad de las instalaciones de procesamiento de la información

3.1. Disponibilidad de los Recursos de Tratamiento de Información.

Con base en el PCN, el Instituto FONACOT elabora una lista de actividades. Estas actividades son clasificadas en una de las siguientes tres categorías:

- Críticas por tiempo: actividades que deben ser reanudadas en menos de 4 horas.
- Críticas: actividades que deben ser reanudadas en menos de 2 días.
- No-críticas: actividades que pueden ser suspendidas por más de 2 días.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Con una mayoría de actividades críticas por tiempo deben considerar desarrollar una solución de recuperación de desastres. Solo actividades críticas (Definido por tiempo e impacto negocio) deben ser tomadas en cuenta para la elaboración del PCN.

3.1.1. Inventario de Recursos de Actividades Críticas.

Se deben identificar todos los recursos necesarios para reiniciar las actividades clasificadas como críticas por tiempo y críticas. Esto implica nombrar personal, identificar los servicios de TI requeridos, conseguir información relativa a equipo especial o herramientas, reunir referencias a archivos en papel, manuales, material de referencia, etc. El administrador del programa debe revisar los resultados del análisis y clasificación de actividades y del inventario de recursos de actividades críticas.

3.1.2. Estrategias de Continuidad de Negocio.

Se deben considerar tres estrategias básicas cuando se desarrolle el PCN:

- Negocio como necesario: para reanudar las actividades sensibles al tiempo a un nivel de normalidad dentro de cuatro horas, una solución de recuperación a desastres debe haber sido establecida, o se necesita de un acuerdo con alguna otra unidad de negocio.
- Negocio para sobrevivir: usar los medios apropiados para reanudar todas las actividades críticas en un periodo de dos días después de la interrupción al negocio.
- Salida ordenada: término temporal del negocio o reubicación de las actividades del Instituto FONACOT. Esta opción puede ser preferida para actividades de bajo volumen y no-críticas.

La elección de estrategia debe ser seleccionada de acuerdo con la criticidad de las actividades y el costo – beneficio de la implementación de esta.

4 PROCEDIMIENTOS ADMINISTRATIVOS.

4.1. Auditoría de Continuidad de Negocio.

Las auditorías internas deben revisar la exactitud y el cumplimiento de los planes de recuperación. Los resultados deben ser revisados para verificar que estén completos.

4.2. Disponibilidad de Planes de Continuidad de Negocio.

El PCN y el DRP, deben ser publicados y distribuidos de forma que aseguren su pronta disponibilidad en caso de que necesiten ser ejecutados por algún incidente.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

15. POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

Esta política para la seguridad de información tiene como objetivo definir y establecer los principales requerimientos para la seguridad física de la información y la tecnología de información dentro del Instituto FONACOT.

2. INVENTARIO DE ACTIVOS.

El Inventario de los Activos de Información debe incluir todos los activos de información.

3. EVALUACIÓN DE RIESGOS AMBIENTALES Y FÍSICOS.

Las medidas físicas de seguridad varían dependiendo de los riesgos de seguridad identificados, las operaciones, así como los atributos de confidencialidad, integridad y disponibilidad de los activos.

Como parte de la evaluación de riesgos se consideran aquellos que están relacionados con la seguridad física y desastres naturales que pueden afectar a los activos, el resultado está orientado a identificar las medidas de seguridad necesarias para procurar niveles aceptables de riesgo.

Los riesgos abordados en la valuación deben incluir:

- Incendio.
- Inundación.
- Explosión.
- Disturbio civil.
- Riesgos que surgen de amenazas naturales específicas a la localidad, ejemplo: terremotos, huracanes.
- Riesgos que surgen de desastres provocados por el hombre, ejemplo: incendio premeditado, actos terroristas.
- Riesgos que surgen de instalaciones cercanas.
- Perímetro de Seguridad.

Una instalación de cómputo es cualquier área que aloja una o más computadoras operativas del Instituto FONACOT, ejemplo: conectadas a una toma eléctrica activa, conectada a una red, etc.

Un perímetro de seguridad se establece creando varias barreras físicas alrededor de los establecimientos e instalaciones que procesan información. Las instalaciones de cómputo del Instituto FONACOT que alojan computadoras que procesan, almacenan o transmiten información clasificada como confidencial se deben localizar dentro de un perímetro de seguridad definido.

Los siguientes requerimientos se deben aplicar a la definición de un perímetro de seguridad:

- El perímetro definido debe estar dentro de una sola estructura o grupo de estructuras vinculadas.
- No debe haber espacios vacíos en el perímetro que proporcionen un medio sencillo de comprometer el perímetro.
- Todas las aperturas del perímetro (ejemplo: puertas, entradas, ventanas) deben estar adecuadamente protegidas y contar con dispositivos que alerten sobre una posible entrada utilizando la fuerza o cualquier actividad sospechosa.
- Debe haber un área de recepción y otros medios de control de acceso físico.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

4. ÁREAS DE SEGURIDAD.

Un área resguardada puede ser una oficina, cuarto o piso completo de cuartos dentro de un perímetro de seguridad física. Los equipos de cómputo y cualquier otro equipo de procesamiento de datos que manipulan, almacenan o transmiten información confidencial deben estar en un área segura.

El área asegurada dentro de una instalación debe proporcionar lo siguiente:

- Acceso restringido.
- Estar en una zona donde no haya acceso al público.
- El equipo de apoyo debe estar ubicado de tal manera que minimice cualquier exposición a información importante.
- Las instalaciones administradas por el Instituto FONACOT deben estar físicamente separadas de las instalaciones administradas por terceros.
- Los directorios, guías telefónicas y mapas del edificio que indican la ubicación de las instalaciones de procesamiento de información no deben tener un acceso sencillo al público.
- Los materiales riesgosos o explosivos nunca deben almacenarse en un cuarto de servidores o en un cuarto de cableado y deben almacenarse a una distancia segura de las instalaciones de procesamiento de información.
- Las instalaciones y equipo de tecnología de información que alojan información del Instituto FONACOT deben estar físicamente protegidas contra el acceso no autorizado, daño e interferencia. Estas instalaciones tienen que estar protegidas por un perímetro físico definido, con controles de entrada y barreras de seguridad apropiadas.
- Se debe contar con equipo contra incendios (extintores, detectores de humo), aire acondicionado, energía regulada en las instalaciones. Estos equipos deben recibir mantenimiento anual para su buen funcionamiento.
- Se debe revisar las instalaciones de agua, gas, calefacción, luz de forma periódicamente para prevenir las fallas o posibles riesgos al Instituto FONACOT.
- Se debe capacitar al personal relacionado con la protección civil.

5. TRABAJO EN ÁREAS SEGURAS.

- Todos los establecimientos que no sean oficinas individuales, instalaciones que alojan computadoras u otros componentes procesadores de información que manipulan, almacenan o transmiten información confidencial deben contar con al menos dos personas autorizadas, siempre y cuando cuenten con personal laboral.
- Los terceros que no han cumplido con los acuerdos de confidencialidad y el reconocimiento de responsabilidades solo pueden recibir acceso limitado y desempeño de actividades supervisadas en áreas seguras.
- El equipo fotográfico, de video u otro equipo para grabar, no está permitido en las áreas aseguradas a menos que se cuente con autorización previa.

6. SEGURIDAD DEL EQUIPO.

6.1 Manejo y Protección de Equipo Asignado al Personal Laboral del Instituto FONACOT.

- El equipo debe estar protegido de amenazas de seguridad y riesgos ambientales.
- El equipo de TI (incluyendo equipo usado fuera de la oficina), equipo de comunicación, computadoras de escritorio y equipo de TI periférico (incluyendo fax, copiadoras y equipo de comunicación) debe estar protegido físicamente para reducir el riesgo de accesos no autorizados a información asegurada y protegerlo contra pérdida o daño.



- El equipo portátil que sale de las instalaciones del Instituto FONACOT no debe dejarse solo en lugares públicos. Cuando el personal viaje, debe llevar la computadora portátil como equipaje de mano y ocultar cuando sea posible. Si el personal no usa el equipo portátil o no está al pendiente de él, debe guardarlo bajo llave.
- Los monitores de computadora que despliegan información confidencial no deben estar ubicados frente a ventanas o puertas. Siempre que sea posible, las computadoras u otros componentes que alojan procesan o transmiten información confidencial deben estar aisladas físicamente de otro equipo, ejemplo: ubicada en una repisa separada.
- También se debe poner atención a la reubicación y al retiro del equipo. Se deben tomar medidas especiales para protegerlo de peligros o accesos no autorizados y proteger las instalaciones que soportan la infraestructura, tales como suministros eléctricos y cableados.
- Se deben aplicar controles para minimizar el riesgo que surge de amenazas potenciales, tales como:
 - Robo.
 - Incendio.
 - Explosión.
 - Humo.
 - Agua.
 - Polvo y otros contaminantes.
 - Inundación.
 - Vibración.
 - Efectos químicos, incluyendo vapores.
 - Interferencia de suministros eléctricos.
 - Radiación electromagnética.
- Toda la información contenida en dispositivos de almacenamientos (tales como discos duros, USB, cintas magnéticas, etc.) que contengan información confidencial deben resguardarse en gavetas o cajoneras bajo llave.
- La DIT debe monitorear las condiciones ambientales. Las condiciones que pudieran tener un impacto en el equipo de procesamiento de datos o medios de almacenamiento deben reportarse inmediatamente.

6.2 Centro de Datos.

- El centro de datos del Instituto FONACOT debe contar con controles que eviten el acceso no autorizado al equipo de cómputo.
- Los centros de cómputo, cuartos de servidores y cuartos de cableado deben ubicarse de modo que los riesgos que surgen de amenazas físicas, tales como incendio o inundaciones, se reduzcan a un nivel aceptable.
- Las puertas de los cuartos de servidores, cuartos de cableado y centros de cómputo deben estar cerradas cuando no haya nadie a través de mecanismos aprobados por el área responsable.
- Dentro del centro de datos se debe contar con cableado eléctrico y de telecomunicaciones separado, de tal manera que evite interferencias, los cables deben estar etiquetados.
- El centro de datos debe contar con alumbrado de emergencia, controles de supresión de picos, una fuente de energía ininterrumpida (UPS).
- Los mantenimientos de los equipos deben realizarse con previa notificación al personal laboral y realizarse únicamente por el personal laboral de mantenimiento autorizado.
- Todo el equipo o mobiliario, propiedad del Instituto FONACOT, que requiera ser trasladado o retirado, debe contar con un memorándum de salida autorizado y firmado por el titular.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- En caso de que un tercero traslade o manipule equipo físico, debe resguardar el equipo de exposición ambiental y de robo, se debe realizar un registro de la cadena de custodia de los equipos, manteniendo los nombres de los responsables.
- Se debe establecer el límite de tiempo en el que el equipo de cómputo se encuentra fuera de las instalaciones y posteriormente verificar su integridad física y digital.

6.3 Seguridad del Cableado.

El cableado de los suministros y de las telecomunicaciones debe estar protegido de ser intervenido o dañado. Las valuaciones de riesgos deben considerar el uso apropiado de los siguientes controles:

- Los cables de suministros y telecomunicaciones deben estar enterrados siempre que sea posible; cuando no se pueda, la valuación de riesgos debe sugerir una protección alterna.
- Los cables de energía deben estar separados de los cables de telecomunicaciones.
- En lo que respecta a los cables que transportan información confidencial, se debe considerar el uso de conductos de cables acorazados o cableado de fibra óptica.
- Se realiza un proceso de limpieza rutinario para eliminar dispositivos no autorizados que se encuentran unidos o sujetos al cableado.

6.4 Mantenimiento del Equipo.

- Se debe dar mantenimiento al equipo de cómputo y a los dispositivos de control ambiental que soportan la información confidencial, de uso interno y la operación del negocio, esto de acuerdo con el procedimiento de mantenimiento preventivo a equipo y al calendario de mantenimiento.
- El mantenimiento del equipo debe realizarse en sitio por personal autorizado siempre que sea posible. Si el mantenimiento o reparación es realizado de manera remota, el Instituto FONACOT debe tomar las medidas de control necesarias para garantizar la confidencialidad e integridad de la información que se tenga almacenada en ese equipo.
- Cada mantenimiento que se le realiza al equipo debe ser adecuadamente registrado y documentado en el reporte de mantenimiento preventivo a equipo.
- El mantenimiento a equipos de cómputo e infraestructura debe realizarse de acuerdo con las recomendaciones del fabricante.
- Se deben llevar registros de todas las fallas, ya sea de las que se tiene sospecha o las que están presentes, así como todo el mantenimiento preventivo o correctivo.
- El equipo que se saque de las instalaciones para darle mantenimiento debe eliminarse, o bien cambiar de clasificación, antes de ser enviado a reparación.

6.5 Reutilización o Eliminación Segura de Equipos.

- Se debe realizar el borrado seguro de los equipos de cómputo que contengan información confidencial del Instituto FONACOT, cuando se requiera el reutilizamiento o destrucción del equipo.
- Cuando el equipo de cómputo se encuentre dañado o sea desechado, se debe realizar una destrucción física del dispositivo.

7. DISPOSICIÓN DE LAS LLAVES DE LAS INSTALACIONES.

Se deben seguir los procedimientos para sacar y monitorear las llaves de las instalaciones que guardan activos de información del Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

16. POLÍTICA DE USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPO DE CÓMPUTO.

1. INTRODUCCIÓN.

Los dispositivos de almacenamiento extraíble (memorias USB, adaptador Bluetooth USB, discos duros portátiles, tarjetas de memoria, CD, DVD, etc.) permiten una transferencia rápida y directa de información. Hoy en día son muy utilizados, y se deben aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus.

Adicionalmente, todo funcionario está obligado a proteger los datos personales de los clientes que estén bajo su custodia e impedir el uso, sustracción, divulgación, alteración, mutilación, destrucción total o parcial de los datos en custodia, tal como lo marca la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

2. ALMACENAMIENTO EN DISPOSITIVOS EXTRAÍBLES.

2.1. Políticas Generales.

La aprobación de las solicitudes para la habilitación de puertos USB de los equipos del Instituto FONACOT, corresponde a cada Subdirección General a la que pertenece el área usuaria de la que proviene cada una de las solicitudes.

El Instituto FONACOT dará seguimiento al cumplimiento de las siguientes directrices.

- Está prohibida la conexión de dispositivos de almacenamiento extraíbles en los equipos de cómputo del Instituto FONACOT, con la finalidad de anular la posibilidad de utilizar los puertos USB, se realizará el bloqueo de estos. Se considera que puedan existir excepciones justificadas, por lo que estas deben solicitarse y aprobarse conforme al Procedimiento de Bloqueo y Desbloqueo de Puertos USB.
- No se podrá bajo ningún caso almacenar datos personales de clientes e información del Instituto FONACOT clasificada como "Confidencial" conforme a Política de Gestión de Activos de Información.
- Queda prohibido transferir información proveniente de clientes y/o proveedores hacia el Instituto FONACOT a través de dispositivos de almacenamiento extraíbles, para transferir información hacia el Instituto FONACOT, se deben utilizar las herramientas Institucionales (correo electrónico, File Server o FTP Server).
- Queda prohibido extraer información confidencial del Instituto FONACOT mediante dispositivos de almacenamiento extraíbles conforme a lo indicado en la política de gestión de activos de información, por lo que estas transferencias de información se deben realizar a través del uso del correo electrónico institucional, File Server o FTP Server.
- Toda la información que se extraiga de los equipos de cómputo y se almacene en dispositivos extraíbles, se considera propiedad del Instituto FONACOT.
- Queda estrictamente prohibido hacer uso de los recursos tecnológicos proporcionados por el Instituto FONACOT con fines distintos a los intereses de este.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

17. POLÍTICA DE ACCESO CON CUENTA PRIVILEGIADA.

1. INTRODUCCIÓN.

Debido al conocimiento operativo y al nivel de acceso a los sistemas e infraestructura de tecnologías de la información del Instituto FONACOT, las cuentas con acceso privilegiado se encuentran en una posición única de confianza y responsabilidad. El acceso privilegiado permite realizar acciones de administración que pueden modificar los activos del Instituto FONACOT, tales como los sistemas operativos, aplicativos, herramientas, redes, accesos, bases de datos y procesos tecnológicos. Una cuenta con acceso privilegiado puede asignarse al personal laboral del Instituto FONACOT o al personal de un proveedor contratado para prestar servicios relacionados con un contrato de servicio vigente.

2. ACCESO CON CUENTA PRIVILEGIADA.

El proveedor de los servicios administrados debe ser el custodio de las cuentas privilegiadas que se generen y/o utilicen en la instalación, operación, administración y cualquier otro apartado que sea referente a la naturaleza de los servicios prestados al Instituto FONACOT.

Los controles de seguridad de la información respecto a los servicios prestados por los proveedores deben apegarse a los lineamientos establecidos en el MGSÍ, dichos lineamientos dan cumplimiento a normas y regulaciones Internacionales a las cuales está alineado el Instituto FONACOT. Por este motivo, los controles que correspondan a los servicios del proveedor deben estar implementados, operando, generando y recolectando la evidencia que sustente la efectividad de estos.

El proveedor debe generar y mantener actualizada una relación de los miembros de su equipo de trabajo que tienen asignada una cuenta con accesos privilegiados. En caso de baja, cambio o reasignación de las cuentas privilegiadas, el proveedor debe notificar de manera inmediata al administrador del servicio y este a su vez al RSI.

El proveedor debe notificar por escrito al administrador del contrato o personal designado las cuentas privilegiadas que tenga bajo su resguardo, además el administrador del contrato debe realizar una revisión mensual de la actividad de las cuentas con acceso privilegiado y presentar un reporte al RSI

La administración de las cuentas privilegiadas se debe realizar y documentar conforme al PROCEDIMIENTO DE GESTIÓN DE CUENTAS en el cual se indican los pasos y actividades específicas.

El proveedor debe elaborar y proporcionar al Instituto FONACOT un informe del manejo general del uso de las cuentas con acceso privilegiado, justificando su utilización, con la finalidad de que el administrador de servicio pueda realizar las validaciones correspondientes, la periodicidad del reporte es mensual o por evento especial.

Cuando el proveedor haga uso inadecuado de cuentas privilegiadas y esto afecte el patrimonio del Instituto FONACOT, se deben dictaminar las penalizaciones correspondientes conforme al contrato de servicio y sus anexos.

Al término de la relación laboral entre el proveedor y el Instituto FONACOT, bajo acto protocolario y entrega/recepción implícita, el proveedor debe entregar al administrador del contrato o personal designado, la relación de cuentas privilegiadas y las contraseñas correspondientes.

- La SGTIC debe tener una cuenta con privilegios de administrador en todos los aplicativos y bases de datos con la finalidad de poder deshabilitar cuentas cuando el contrato de los proveedores haya terminado.
- El proveedor debe elaborar y proporcionar al Instituto FONACOT un informe del uso de las cuentas con acceso privilegiado, justificando su utilización. El administrador del servicio debe realizar las validaciones correspondientes, la periodicidad del reporte es mensual o por solicitud especial.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
Vigencia: Julio, 2024			

El Instituto FONACOT se reserva el derecho de poder realizar en cualquier momento inspecciones en sitio y/o a documentación en general y evidencia, acerca del diseño de los controles, funcionalidad y eficiencia de estos. Estas revisiones pueden ser realizadas directamente por el Instituto FONACOT o a través de un tercero.

Las cuentas privilegiadas deben tener asignada una MAC Address de manera que no puedan ser utilizadas en otro equipo diferente al asignado.

El RSI solicitará periódicamente las bitácoras de acceso y registro del uso de las cuentas con acceso privilegiado y en caso de identificarse anomalías se deben emprender las acciones correspondientes.

2.1. Sistemas Operativos.

El responsable de la administración del servicio debe solicitar la generación de cuentas privilegiadas de los sistemas operativos al proveedor de infraestructura.

Las cuentas privilegiadas deben ser generadas y asignadas por el proveedor de infraestructura al responsable del aplicativo que designe el proveedor, informando al administrador del servicio solicitante perteneciente al Instituto FONACOT.

2.2. Aplicaciones y Cuentas de Servicio.

El proveedor responsable de la administración del aplicativo debe informar de manera mensual o por algún evento especial al administrador del servicio por parte del Instituto FONACOT las cuentas de servicio generadas para la propia operación y/o administración del aplicativo correspondiente.

El proveedor responsable de la administración del aplicativo será responsable de la custodia y uso de las cuentas de servicio.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

18. POLÍTICA DE CONEXIONES VPN (RED PRIVADA VIRTUAL) CLIENTE – SERVIDOR.

1. INTRODUCCIÓN.

Debido a la necesidad de operación del Instituto FONACOT con los servicios de Tecnologías de la información, se requiere la conexión remota de manera segura para el acceso a los sistemas Institucionales, servicios informáticos y administración de infraestructura y aplicativos.

2. CONEXIONES VPN (RED PRIVADA VIRTUAL) CLIENTE – SERVIDOR.

El personal laboral aprobado por el Instituto FONACOT y terceros autorizados (clientes, proveedores y otros) pueden utilizar el servicio de conexiones VPN, para lo cual deben considerar los siguientes puntos:

- El personal debe contar con un servicio de internet y contar con las configuraciones necesarias en su computadora para establecer conexión con el Servidor de Acceso Remoto.
- Es responsabilidad de la DIT asegurar que las cuentas sin autorización del servicio de conexiones VPN, tengan deshabilitado este servicio.
- La autenticación de personal que establezca una conexión VPN será mediante una cuenta de dominio y contraseña. Por lo que, es importante atender los lineamientos de contraseña de la Política de Control de Accesos.
- Solo se permite una conexión de VPN por persona.
- Las puertas de enlace VPN son configuradas y administradas por los grupos operativos de la red del Instituto FONACOT y son asignadas al equipo del personal a través de DHCP.
- A través de la conexión VPN únicamente se permitirá el acceso al servidor, aplicación y/o servicio requerido, situación que debe estar justificada ampliamente.
- A través de las conexiones VPN no estará permitido el escaneo de redes y/o ejecución de análisis de vulnerabilidades.
- Queda prohibida la extracción de cualquier tipo de información visualizada o recabada del Instituto FONACOT.
- Toda computadora que establezca una conexión VPN debe contar con software de antivirus actualizado y parches de seguridad actualizados.
- Las conexiones VPN se desconectan automáticamente después de treinta minutos de inactividad. Pasado este tiempo se debe iniciar sesión nuevamente para volver a conectarse a la red. Los pings u otros procesos de red no deben usarse para mantener la conexión abierta.
- Cualquier conexión de VPN está limitada a un tiempo de vida absoluto de 24 horas.
- Las computadoras que no son propiedad del Instituto FONACOT deben ser configuradas para cumplir con las políticas de red, seguridad y conexión VPN establecidas por el Instituto FONACOT.
- Al utilizar una conexión VPN con computadoras personales, el personal debe comprender que sus equipos son una extensión de la red del Instituto FONACOT y como tal, están sujetas a las mismas reglas y regulaciones establecidas para las computadoras del Instituto FONACOT. Los equipos deben configurarse para cumplir con las políticas de seguridad del Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

19. POLÍTICA DE CORREO ELECTRÓNICO.

1 INTRODUCCIÓN.

El correo electrónico se usa de forma generalizada y es uno de los principales canales de comunicación dentro del Instituto FONACOT, al ser un medio por el cual se comparte información, se debe garantizar la privacidad de los datos personales y la seguridad de la información.

El propósito de esta política es proporcionar los elementos para el uso adecuado del correo electrónico del Instituto FONACOT.

2 REQUISITOS DE SEGURIDAD EN EL USO DE CORREO ELECTRÓNICO.

El servicio de correo electrónico del Instituto FONACOT debe considerar al menos lo siguiente:

- La inserción de una leyenda de confidencialidad de la información en los correos emitidos.
- El control sobre la totalidad de los correos electrónicos.
- Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso.
- Comprobar que los correos electrónicos fueron enviados y autorizados por un emisor válido y determinar la autenticidad del contenido de los mensajes de correo electrónico a través de los protocolos DMARC, SPF y DKIM.
- Uso de mecanismos de cifrado de la información.
- Configuración del envío y recepción de correos electrónicos para restringir la entrada y salida hacia dominios públicos o privados diferentes a los autorizados.
- El Instituto FONACOT debe contar con los elementos para acceder y tener a su disposición la totalidad de los correos electrónicos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

20. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN BASES DE DATOS.

1. INTRODUCCIÓN.

El Instituto FONACOT está consciente que en los últimos años los incidentes de seguridad relacionados con la confidencialidad de la información se han producido con mayor frecuencia, aunado a la naturaleza de los servicios que presta. Esto hace que gran parte de la información crítica sea sustentada por bases de datos, lo que resalta la necesidad de contar con seguridad de la información en bases de datos.

2. SEGURIDAD DE LA INFORMACIÓN EN BASES DE DATOS.

2.1. General.

La seguridad en las bases de datos del Instituto FONACOT debe considerar a quienes tendrán acceso, a que información y de qué manera, contemplando la confidencialidad, integridad y disponibilidad de la información.

El Instituto FONACOT debe contar con tecnologías (WAF-DBF) que proporcionen protección de la base de datos en tiempo real contra amenazas internas y externas a través de alertas o bloqueo de ataques y solicitudes de acceso anormales.

2.2. Clasificación de Información.

El Instituto FONACOT, identificará y clasificará la información que debe ser protegida según su importancia, conforme a lo indicado en el marco jurídico administrativo que rige al MGSI.

2.3. Configuración Inicial.

2.3.1. Instalación.

Uso de Últimas Versiones.

El Instituto FONACOT debe tener instalada la última versión estable de DBMS soportada por la aplicación y plataforma que esté disponible, así como los respectivos parches de seguridad.

Para ello se deben realizar al menos las siguientes acciones:

- **Identificación de activos y software:** Se debe llevar a cabo la identificación de servidores y bases de datos instaladas, así como el nivel de parches de seguridad aplicados, de manera que los cambios se realicen sin riesgos y en caso de producirse algún problema en la actualización o aplicación de parches de seguridad, se permita volver a un estado previo conocido y funcional.
- **Disponibilidad:** Se debe tener un inventario actualizado de servidores y bases de datos, adicionalmente se debe revisar el listado de actualizaciones y parches de seguridad disponibles e identificar cuál de ellos afecta a cada servidor y base de datos.
- **Aplicabilidad:** Las actualizaciones y parches de seguridad publicados no siempre son válidos para todos los equipos, por lo que se debe verificar si la actualización o parche de seguridad son viables.
- **Adquisición:** Se deben obtener los archivos de actualización, así como los parches de seguridad de una fuente confiable.
- **Validación:** Asegurar que la actualización y/o aplicación de parches no impacta de manera negativa la confidencialidad, integridad o disponibilidad de los sistemas de información. Para tal efecto se deben realizar comprobaciones sobre las implicaciones de la actualización o aplicación de parches de seguridad.
- **Despliegue:** Durante el proceso de validación se debe crear un paquete de despliegue. El paquete debe contener el/los archivos de actualización o parches y las instrucciones de instalación, así como un listado de los servidores y bases de datos en los que realizará el despliegue.

Instalar Funcionalidad Mínima.

Para minimizar el riesgo de accesos no autorizados, así como hacer uso correcto de recursos, se debe seleccionar e instalar sólo las funcionalidades requeridas, las funcionalidades que no son necesarias, pero instaladas como predeterminadas, deben eliminarse o deshabilitarse.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Cambio de la Configuración de Puertos.

Para reducir la probabilidad de accesos no autorizados, se deben cambiar los números de puerto que son ampliamente utilizados o configurados por defecto durante la instalación.

Restringir el Acceso a la Red.

Para evitar el uso no autorizado de las funciones de red, se debe restringir el acceso a las funciones de acceso a la red de DBMS.

2.4. Autenticación.

2.4.1. Gestión de cuentas.

Evitar la Creación de Cuentas Innecesarias.

Para evitar la suplantación por el uso no autorizado de la información de cuentas, se deben crear sólo las cuentas que sean justificadas y autorizadas por los responsables de la base de datos.

El Instituto FONACOT, debe contar con el listado de los roles aplicables a las cuentas de la base de datos y los privilegios asignados a cada una de ellas.

Debe existir una adecuada segregación de funciones y privilegios, respecto a las cuentas de la base de datos (cuenta externa, cuenta interna, cuenta de la aplicación (por cada aplicación), administrador de la base de datos, operador de base de datos, etc.)

Eliminación y Bloqueo de Cuentas.

Se deben eliminar las cuentas que no están en uso, debido a que hayan causado baja o transferencia a otras funciones que ya no justifique el uso de la cuenta, también deben borrarse las cuentas predeterminadas que no se utilizan.

Se deben bloquear las cuentas que se han utilizado sólo una vez en un año, así como las cuentas que tengan 5 intentos de inicio de sesión fallidos de manera consecutiva.

Gestión de Cuentas de Administrador de Base de Datos.

Las cuentas con permisos elevados (Administradores) de la base de datos, sólo se asignan al personal que lo justifique. Por cada asignación debe existir una responsiva firmada, las responsivas quedan bajo el resguardo de la DTI.

Deben habilitarse las pistas de auditoría que documente las actividades realizadas a través de las cuentas con permisos elevados, estos registros deben ser resguardados por la DTI, además de ser notificados de manera periódica al RSI.

Las cuentas de administrador de la base de datos no se deben utilizar en actividades que no requieran privilegios de administrador.

Se debe asignar una cuenta única de administrador de la base de datos a cada administrador, por lo que está prohibido compartir estas cuentas.

Otros Lineamientos Respecto a Cuentas.

En la configuración inicial de las cuentas se debe limitar la capacidad de tener sólo una sesión abierta, en caso de ser necesario y requerir más de una sesión de manera simultánea debe justificarse y ser autorizada por el responsable de la base de datos, esta excepción debe ser documentada y considerada en la revisión periódica de registros.

En la configuración inicial de las cuentas se debe limitar el tiempo de inactividad a 30 minutos antes de ser desconectada. En caso de requerirse otro parámetro, este debe ser justificado y autorizado por el responsable de la base de datos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.5. Control de Acceso.

2.5.1. Configuración de Privilegios de Acceso.

Determinación de los Requisitos de Acceso a la Base de Datos.

Para que los controles de acceso se asignen adecuadamente, se deben clasificar las cuentas según sus propósitos y usos (administradores de base de datos, administradores de objetos, acceso a datos, etc.), así como definir los privilegios de acceso necesarios para cada clasificación de cuenta, detallando la funcionalidad, ruta de conexión de acceso, acceso a objetos, etc.

Las cuentas deben ser divididas según los privilegios, para cada una de estas cuentas se determinará el rango mínimo de datos necesarios para acceder y los privilegios mínimos (lectura, escritura, creación y eliminación) que deben establecerse, así como los requisitos de acceso a la base de datos.

2.5.2. Establecer Privilegios de Acceso.

Para restringir el acceso a los datos, se deben asignar los privilegios mínimos de acceso necesarios para cada cuenta. Los privilegios de administrador se asignan a un número limitado de cuentas autorizadas previamente por el responsable de la base de datos.

2.5.3. Revisión de Acceso.

El RSI solicitará periódicamente las bitácoras de acceso, el cual tomará las acciones que correspondan.

2.6. Revisión de Cuentas de Acceso.

Para que los privilegios se apliquen de manera correcta, estos se deben comprobar periódicamente para asegurarse que no se otorguen privilegios innecesarios, así también se deben revisar los privilegios de las cuentas cuando se hayan aplicado cambios a los sistemas y cuando dentro del contexto de operación cotidiana se descubran cuentas con privilegios innecesarios.

2.7. Cifrado.

Para que los datos almacenados en la base de datos estén protegidos contra el robo, se debe implementar un cifrado en los datos almacenados, archivos físicos y copia de seguridad utilizando funciones o herramientas de cifrado.

De manera adicional, se deben seguir los lineamientos establecidos en la Política de Criptografía.

2.8. Otros.

2.8.1. Rutas de Acceso a Archivos.

Limitar el Acceso a los Archivos de Configuración de la Base de Datos.

Para evitar la destrucción de la base de datos, los derechos de acceso a los archivos de configuración de la base de datos deben revisarse periódicamente y sólo los administradores pueden tener acceso a los archivos de configuración de la base de datos y a los archivos de script.

Limitar las Rutas de Conexión.

Para evitar errores operativos y el uso no autorizado de la base de datos, las aplicaciones (incluidas las herramientas de administración) utilizadas para acceder a la base de datos deben instalarse sólo en las PC autorizadas, además se deben restringir las rutas de conexión de red que pueden usarse para acceder a la base de datos / servidor.

3. DETECCIÓN DE BASE DE DATOS Y CONTROLES DE SEGURIDAD FORENSE.

Se deben generar registros que contengan información adecuada para el monitoreo y análisis forense. La finalidad es identificar y resolver eficazmente los problemas de seguridad.

3.1. Gestión de Registros.

3.1.1. Registro.

Para monitorear el acceso a la información, los registros de productos y actividades relacionadas con el acceso / cambios a información personal, confidencial y otra información considerada como significativa, deben ser

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

documentados, así como los registros de auditoría de objetos de base de datos (por ejemplo, cuentas de base de datos, tablas, vistas, etc.), creación y cambios.

3.1.2. Protección de Registro.

Para que los registros se encuentren disponibles, se deben copiar los registros en medios extraíbles externos, manteniendo una bitácora que al menos contenga la ubicación de almacenamiento, medios de almacenamiento, tiempo de retención y controles de acceso a implementar.

Se debe prevenir la modificación del registro, previniendo modificaciones no autorizadas del registro a través de la retención de múltiples copias en medios de almacenamiento de sólo lectura y utilizar firmas digitales usando marcas de tiempo.

3.2. Detección de Acceso No Autorizado.

Incluso si una base de datos está protegida contra el acceso no autorizado, siempre existe la posibilidad de que esto se intente. Por lo tanto, es necesario contar con un mecanismo para detectar tales intentos.

3.2.1. Mecanismos de detección.

Para detectar el acceso no autorizado, se debe implementar un mecanismo para notificar los intentos de acceso no autorizados y notificar al responsable, administrador y al equipo de respuesta a incidentes que se ha producido un bloqueo de cuenta (debido a que se ha excedido el número máximo de intentos fallidos de inicio de sesión).

3.2.2. Comprobación del Tiempo de Acceso.

Detección de Acceso a la Información de Administración de DBMS.

Para detectar el acceso sospechoso a la información de administración de DBMS durante y fuera del horario laboral, se debe monitorear, detectar y registrar el acceso que está fuera del tiempo autorizado, así como también comprobar que el trabajo realizado es el especificado al comparar el registro y el formulario de solicitud de trabajo.

Detectar Acceso a la Información de la Base de Datos

Para detectar el acceso sospechoso a la información de la base de datos durante y fuera del horario laboral, se deben definir para cada cuenta de la aplicación el tiempo de trabajo en el que está autorizado para acceder al DBMS, así como monitorear el registro de sesión, detectando cualquier acceso que esté fuera del horario de trabajo autorizado.

3.2.3. Comprobación de Otros Accesos No Autorizados.

Para detectar accesos no autorizados, se deben detectar ataques de diccionario, verificando que los intentos fallidos de inicio de sesión sean inferiores a un número predeterminado durante un período de tiempo determinado, monitorear, registrar y detectar la ejecución de SQL, así como la creación de objetos de base de datos y los cambios.

3.3. Análisis de Registros.

Se debe determinar que un evento en particular es una violación de seguridad, analizando los registros desde varios ángulos. Además, los registros documentados anteriormente también deben ser considerados en el análisis.

La finalidad será detectar las brechas de seguridad de los registros de auditoría.

El análisis periódico de la información de la sesión debe contener al menos la siguiente información:

- Fecha y hora (cuándo).
- Base de datos / ID de cuenta de aplicación (Quién).
- ID del objeto, nombre de la tabla (Qué).
- Nombre del host (PC) y dirección IP (Dónde).
- Tipo de SQL y cuerpo / oración de consulta (Cómo).
- Éxito o fracaso del intento de acceso (Resultado).

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

21. POLÍTICA DE CONTROL DE SEGUIMIENTO A VULNERABILIDADES.

1. INTRODUCCIÓN.

El seguimiento a vulnerabilidades de seguridad de la información es un componente crítico en la gestión de la seguridad del Instituto FONACOT, la finalidad de este seguimiento es reducir el impacto a la operación derivado por alguna amenaza que sea explotada por vulnerabilidades presentes en la infraestructura tecnológica, bases de datos o aplicativos del Instituto FONACOT.

La intención es que el Instituto FONACOT tenga un método formal para dar seguimiento a la remediación de vulnerabilidades detectadas por los especialistas de la seguridad de la información, de manera que las correcciones o mejoras puedan ser resueltas correctamente, en tiempo y en forma, permitiendo en todo momento conocer el estado que guarda la atención de dichas vulnerabilidades.

2. SEGUIMIENTO A VULNERABILIDADES.

2.1. Plan Anual de Vulnerabilidades.

El RSI elaborará el plan anual de vulnerabilidades sobre la infraestructura tecnológica, bases de datos, aplicativos web y móviles considerados críticos y debe presentarlo a las áreas involucradas del Instituto FONACOT para su ejecución y seguimiento.

2.2. Proceso de Identificación y Remediación de Vulnerabilidades.

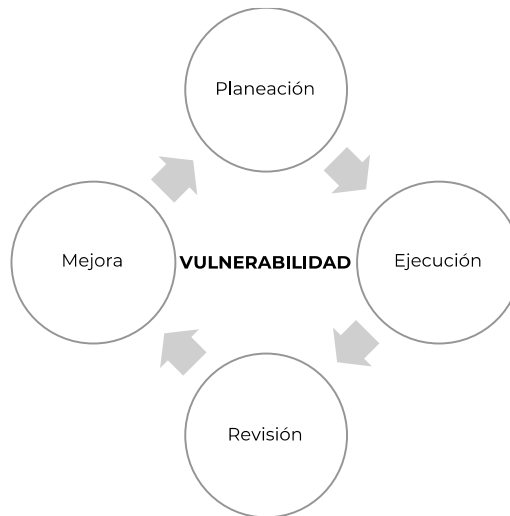
El RSI y las áreas involucradas del Instituto FONACOT realizan las siguientes actividades:

- Seguridad - Realiza actividades de análisis de seguridad a la infraestructura tecnológica con la finalidad de identificar vulnerabilidades.
- Seguridad – Por cada una de la vulnerabilidad detectada se entrega al área involucrada del Instituto FONACOT en cuestión, el detalle, la criticidad y urgencia de corrección, incluyendo recomendaciones de corrección. Cada vulnerabilidad debe contar con un identificador único (ID) a través del cual se lleve a cabo el seguimiento a la atención y remediación del mismo, documentar todo el seguimiento en la bitácora de seguimiento a vulnerabilidades.
- El área involucrada del Instituto FONACOT- Analiza la sugerencia de corrección y demás información recibida por el equipo de seguridad de la información.
- El área involucrada del Instituto FONACOT- Informa la decisión acerca de implementar la solución propuesta por el equipo de seguridad o bien considerar una solución alterna para la vulnerabilidad, justificando los motivos.
- El área involucrada del Instituto FONACOT- Implementa la solución y notifica al equipo de seguridad de la información los resultados.
- Seguridad - Confirma que la solución a la vulnerabilidad ha sido atendida.

2.3. Modelo para el Seguimiento a Vulnerabilidades.

El RSI será el responsable del seguimiento a la remediación de las vulnerabilidades y que han sido reportadas a las áreas involucradas del Instituto FONACOT para su atención.

El seguimiento a las vulnerabilidades considera las siguientes fases:



Planeación – En esta fase el área involucrada del Instituto FONACOT presenta al equipo de seguridad de la información, la estrategia y la planeación para la atención de la incidencia.

El plan debe incluir la fecha de inicio y terminación de la remediación, persona líder y equipo responsable, ruta crítica, criterios de pruebas y aceptación, así como el presupuesto que llegara a ser necesario.

Ejecución – El área involucrada del Instituto FONACOT, llevará a cabo las actividades planificadas necesarias para llevar a cabo la mitigación de la vulnerabilidad.

Revisión – El área involucrada del Instituto FONACOT, debe realizar pruebas unitarias e integrales, así como de estrés y volumen, considerando todos los escenarios bajo los cuales fue detectada la vulnerabilidad.

El encargado de seguridad debe revisar estas pruebas proporcionadas por el área involucrada del Instituto FONACOT, solicitar al equipo de seguridad bajo su mando, la realización de la revisión de la mitigación de la vulnerabilidad y en caso de confirmar la corrección, otorgar su visto bueno.

Mejora – El Instituto FONACOT basa la mejora de su seguridad de la Información, a través del MGSI el cual se basa en el modelo de Mejora Continua “Deming (PHVA)”.

Adicionalmente, el equipo de seguridad realiza un control sobre el seguimiento de las vulnerabilidades con la finalidad de analizar la recurrencia por tipo de vulnerabilidad y el tiempo de atención con relación a la criticidad de la vulnerabilidad.

2.4. Responsabilidades.

El área involucrada del Instituto FONACOT responsable del activo debe mitigar la vulnerabilidad y el RSI entregará los reportes de análisis de vulnerabilidades a los responsables de los activos. Estas vulnerabilidades deben atenderse en un plazo no mayor a 3 meses para las vulnerabilidades críticas y en un plazo no mayor a 6 meses para las vulnerabilidades medianas. En caso de que no se atiendan dichas vulnerabilidades por los responsables de los activos, el RSI levantará un reporte de Riesgos a dichos responsables.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

22. POLÍTICA DE PLANIFICACIÓN DE RESPUESTA ANTE UNA CAUSA DE FUERZA MAYOR O DE CASO FORTUITO.

1. INTRODUCCIÓN.

Los desastres generalmente ocurren dentro de un área geográfica. Un huracán o un terremoto pueden causar daños masivos en un área, sin embargo, el peor daño generalmente se encuentra dentro de unos pocos kilómetros. Una pandemia global, como el brote de influenza de 1918 que infectó a 1/3 de la población mundial, puede tener un alcance de afectación mayor y por ello se requiere de una planificación eficaz de actividades respecto con la arquitectura de TI, conocimiento de la situación, capacitación del personal laboral y otras preparaciones.

Ante una causa de fuerza mayor o de caso fortuito, el Instituto FONACOT puede cerrar oficinas al personal laboral no esencial o cierre total con la finalidad de reducir el riesgo inmediato. Ante tal escenario es necesario contar de forma anticipada con un plan de respuesta que aborde quién puede trabajar de forma remota, cómo son las operaciones e identifica qué otros problemas pueden enfrentar, ayudará al Instituto FONACOT a sobrevivir en un momento en que la mayoría de las personas se preocupan por sí mismas y sus familias.

2. RESPUESTA ANTE UNA CAUSA DE FUERZA MAYOR O DE CASO FORTUITO.

El Instituto FONACOT autoriza, desarrolla y mantiene un Plan de respuesta ante una pandemia que aborde los siguientes puntos:

2.1. Liderazgo.

El liderazgo del plan de respuesta ante una pandemia se identificará como un pequeño equipo que supervisará la creación y actualización del plan. El liderazgo también será responsable de desarrollar experiencia interna en la transmisión de enfermedades y otras áreas como el fenómeno de la segunda ola para guiar los esfuerzos de planificación y respuesta. Sin embargo, como con cualquier otra posición crítica, el liderazgo debe tener suplentes capacitados que puedan ejecutar el plan en caso de que el liderazgo no esté disponible debido a una enfermedad.

2.2. Plan.

La creación de un plan de comunicaciones antes y durante un brote pandémico que explique los servicios de telecomunicaciones que son utilizados.

2.3. Sistema de Alerta.

Un sistema de alerta basado en el monitoreo de la OMS, Secretaría de Salud y otras fuentes de información federales, estatales y locales sobre el riesgo de un brote de enfermedad pandémica.

2.4. Niveles de Respuesta.

Un conjunto predefinido de políticas de emergencia que se adelantará a las políticas normales del Instituto FONACOT durante la duración de una pandemia declarada. Estas políticas de emergencia deben organizarse en diferentes niveles de respuesta que coincidan con el nivel de interrupción que se espera de un posible brote de enfermedad pandémica dentro de la comunidad. Estas políticas deben abordar todas las tareas críticas para la continuación de la operación, incluyendo:

- Dónde trabajará la gente, incluyendo quedarse en casa o traer niños al trabajo.
- Cómo las personas cumplen sus tareas si no pueden presentarse a la oficina.
- ¿Qué trabajo se suspenderá durante la pandemia?
- Plan de comunicación y cadencia a lo largo de la pandemia.
- Medios alternativos para comunicarse durante la pandemia.
- Qué procedimientos operativos pueden necesitar ser alterados, enmendados o suspendidos, tales como los de instalaciones, visitantes y actividades y eventos no esenciales.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.5. Indicadores.

Un conjunto de indicadores para la administración que los ayudará a seleccionar un nivel apropiado de respuesta que ponga en práctica las políticas relacionadas discutidas en la sección 4.4 para el Instituto FONACOT. Debe haber un nivel gradual de respuesta relacionado con el nivel de alerta de pandemia u otros indicadores autorizados de un brote de enfermedad.

2.6. Capacitación y Sensibilización.

Un proceso de capacitación que cubre la protección personal que incluye:

- Identificar y comunicar ampliamente los síntomas de exposición.
- El concepto de grupos de enfermedades en guarderías, escuelas u otras grandes reuniones.
- Prevención básica: limitar el contacto a menos de 1 y medio metros, cubrirse al toser, lavarse las manos, entre otros.
- Cuando quedarse en casa.
- Evitar viajar a todas las áreas con altas tasas de infección.

2.7. Personal Laboral Clave.

Un proceso para identificar al personal laboral clave para cada función crítica y hacer la transición de sus deberes a otros en caso de que se enfermen o no puedan realizar sus respectivos deberes.

2.8. Suministros.

Una lista de suministros que se deben tener a mano o pre contratados para los suministros, como máscaras faciales, desinfectante de manos, combustible, alimentos y agua.

2.9. Problemas Relacionados con TI.

- Asegurar que las áreas críticas consideren contingencias pandémicas en su planificación.
- Verificación de la capacidad tecnológica al aumentar significativamente el trabajo a distancia, incluido el ancho de banda, licencias, la capacidad de ofrecer voz sobre IP y la disponibilidad de computadoras portátiles.
- Mayor uso de herramientas de reuniones virtuales que facilitan las capacidades de videoconferencia y uso compartido de escritorio.
- Identificar qué tareas no se pueden realizar de forma remota.
- Los acuerdos pre negociados con proveedores clave en el caso de que las licencias actuales no cumplan con este cambio en los hábitos de la fuerza laboral.
- Determinar si hay personal laboral de TI que necesita permanecer en sitio para soportar operaciones críticas.
- Planificar las diferentes maneras de cómo el personal interactúa con el Instituto FONACOT.
- Expectativas sobre la impresión de documentos de trabajo en impresoras personales.
- Expectativas sobre la formalización de documentos (firmas).
- Expectativas sobre el envío de correos electrónicos y documentos de trabajo a cuentas de correo electrónico personales.

2.10. Prueba y Actualización del Plan.

La creación de ejercicios para probar el plan de respuesta ante una pandemia.

Realizar una revisión retrospectiva para identificar y resolver los problemas encontrados en la prueba.

El proceso y la frecuencia de las actualizaciones y revisiones del plan al menos una vez al año con las aprobaciones apropiadas o la aprobación del liderazgo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

23. POLÍTICA DE ASIGNACIÓN DE EQUIPO DE CÓMPUTO.

1. INTRODUCCIÓN.

El Instituto FONACOT sustenta sus operaciones a través del uso de tecnologías de la información, en donde sus actividades cotidianas que forman parte del negocio, así como aquellas enfocadas a la automatización de oficinas, hacen uso de equipo de cómputo.

2. ASIGNACIÓN DE EQUIPO DE CÓMPUTO.

El Instituto FONACOT mantiene una estrategia para la asignación de equipo de cómputo al personal laboral del Instituto FONACOT que aborde los siguientes puntos:

2.1. Aprovisionamiento del Equipo de Cómputo.

Se considerará el aprovisionamiento de equipo de cómputo bajo los siguientes rubros:

- Para todo el personal laboral que requiera de un equipo de cómputo para realizar su trabajo diario.
- Para una contratación de nuevo personal laboral que requiera de un equipo de cómputo para realizar sus actividades.
- Para un cambio de puesto y actividades de cualquier elemento del personal laboral que requiera un equipo de cómputo o actualización de este debido a los requerimientos del nuevo puesto.
- Para áreas específicas que por su operación así lo requieran.
- Para equipamiento de salones, laboratorios o salas de cómputo que apoyen al trabajo del Instituto FONACOT.

El aprovisionamiento de equipo de cómputo debe realizarse directamente por el Instituto FONACOT o a través de un proveedor de servicios administrados dedicado a estos servicios.

2.2. Actualización o Reemplazo de Equipo de Cómputo.

La actualización o reemplazo de equipo de cómputo asignado al personal laboral, se sugiere realizar en los siguientes casos:

- Cuando el equipo de cómputo PC (Escritorio o portátil) cuente con tres o cuatro años de uso.
- Cuando el equipo de cómputo Apple Mac (Escritorio o portátil) cuente con cuatro o cinco años de uso.
- En el caso de equipo de cómputo móvil como Tabletas será revisado y dependerá de la obsolescencia del software, proyectos o estado del equipo.

2.3. Recolección o Recepción de Equipo de Cómputo.

La recolección o recepción del equipo de cómputo se llevará a cabo bajo los siguientes escenarios:

- Cuando el personal laboral deja de prestar sus servicios en el Instituto FONACOT.
- Cuando el personal laboral hace cambio de localidad y/o funciones (previa evaluación y justificación).
- Cuando un equipo ya no sea necesario para el trabajo del área.

2.4. Consideraciones.

La asignación o reemplazo del equipo de cómputo al personal laboral dependerá de las actividades que este realice dentro del Instituto FONACOT en acuerdo con la persona líder del área donde el personal laboral desempeñe sus funciones y la Dirección de Recursos Humanos, respetando los criterios de tipo de equipo asignado para tipo de trabajo que el personal realiza.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

La administración, configuración, mantenimiento, actualización y asignación del equipo de cómputo es responsabilidad de la DIT por lo que ningún elemento del personal laboral podrá reasignar o disponer de un equipo de cómputo sin la autorización o acuerdo con la DIT.

La DIT será la responsable de que el equipo de cómputo que opera en el Instituto FONACOT sea el adecuado para cada tarea, cuidando así los recursos y gasto del Instituto FONACOT en este tema, por lo que la compra, actualización y asignación de cada equipo de cómputo, periférico o accesorio debe tener el visto bueno de esta área.

2.5. Niveles de Servicio (SLA).

Asignación de Equipo de Cómputo a Nuevo Personal Laboral.

Inmediato al primer día de labor, siempre y cuando se cubra el proceso pactado en tiempo y forma con Recursos Humanos sobre el aviso y solicitud de equipo de cómputo.


Actualización de Equipo de Cómputo al Personal Laboral.

Se mantiene el equipo de cómputo asignado al personal laboral, departamentos, salones y salas de cómputo en un periodo de 3 a 4 años en el caso de los equipos PC y de 4 a 5 años en equipos Apple MAC ya sea de escritorio o Laptop con las características y poder de cómputo necesario para el desempeño de sus labores.

Reemplazo de Equipo de Cómputo al Personal Laboral o Área en Caso de Pérdida o Daño.

En el caso de pérdida de equipo por robo, extravío o daño físico, se procurará el reemplazo, después de cubrir los procesos necesarios y pactados por parte del personal laboral y el Instituto FONACOT.

- Caso de Robo.
 - Aviso inmediato la Subdirección de Infraestructura Tecnológica y Dirección de Recursos Humanos.
 - Entrega de la copia del acta ministerial que consta la denuncia del robo.
 - Disponibilidad de un equipo para sustituir al robado.
- En el caso por daño físico a causa del mal uso o maltrato al equipo.
 - Aviso por parte del personal laboral a la Subdirección de Infraestructura Tecnológica y Dirección de Recursos Humanos.
 - Pago de las partes o refacciones que el equipo necesite para seguir funcionando correctamente o el pago correspondiente del equipo en el caso de que el equipo quede irreparable.
- En el caso específico de la reparación del equipo, este se entregará al personal laboral hasta ser reparado y configurado por la Subdirección de Infraestructura Tecnológica.
- En el caso de daño parcial o total después de un uso normal de trabajo y debido a problemas electrónicos ajenos a la persona usuaria u operación, la reposición corre a cargo de la Subdirección de Infraestructura Tecnológica y el tiempo de reposición dependerá de la disponibilidad del equipo a sustituir.
- En el caso de la pérdida o daño de un equipo de cómputo clave o prioritario para operaciones del Instituto FONACOT.
 - Aviso por parte del personal laboral responsable de la Subdirección de Infraestructura Tecnológica.
 - La reposición será inmediata y seguida de los procedimientos mencionados en los puntos anteriores.
 - En el caso de no contar con un equipo con las características necesarias, se gestionarán los trámites necesarios para su reemplazo a la brevedad posible, buscando alternativas temporales para no afectar la operación inmediata del área.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.6. Uso del Equipo de Cómputo.

El personal laboral del Instituto FONACOT debe utilizar exclusivamente el equipo de cómputo propiedad de la dependencia o arrendado para el desempeño de sus actividades laborales.

La instalación o reubicación del equipo al interior de una misma área, ya sea independiente o conectado a la red, será realizada únicamente por personal laboral de la Subdirección de Infraestructura Tecnológica.

La DIT debe elaborar y mantener actualizado el registro de la distribución y asignación del equipo de cómputo.

2.7. Control de Acceso.

Cada equipo de cómputo debe tener una cuenta y contraseña para el acceso al mismo, la cual únicamente será de conocimiento de la persona asignada y esta no debe ser compartida.

La estructura de una contraseña debe apegarse a los lineamientos indicados en Procedimiento de Contraseñas.

2.8. Seguridad Física del Equipo de Cómputo.

No se debe fumar ni ingerir alimentos o bebidas al hacer uso de los equipos de cómputo.

Queda prohibido conectar aparatos o equipos que no sean computadoras a los tomacorrientes regulados y fuentes interrumpibles de energía.

Los equipos deben estar apagados antes de ser conectados o desconectados del tomacorriente o de los puertos de red, así como para efectuar cualquier mantenimiento, instalación o actualización de estos.

La DIT revisará periódicamente que el equipo se encuentra en las mismas condiciones físicas en las que se asignó a la persona (bancos de memoria, disco duro, unidades de cd, etc.), lo anterior con la finalidad de detectar posible extracción de algún componente interno o externo del equipo.

2.9. Uso del Equipo de Cómputo.

- No se debe instalar ni hacer uso de programas de cómputo sin la licencia de uso correspondiente.
- No se debe instalar programas que no tienen aplicación en las funciones propias del Instituto FONACOT.
- Todo equipo debe tener instalado un programa de antivirus debidamente actualizado.
- La DIT debe realizar un mantenimiento preventivo mínimo una vez al año al equipo de cómputo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

24. POLÍTICA DE BORRADO SEGURO.

1. INTRODUCCIÓN.

El Instituto FONACOT al ser una institución de crédito se clasifica dentro del sector financiero y por lo tanto está obligada a dar cumplimiento regulatorio respecto con la gestión de información del Instituto FONACOT, así como del tratamiento y seguridad de datos personales.

El Instituto FONACOT debe mantener un ciclo de vida de la información, la cual consta de tres fases:

- a) Generación
- b) Transformación
- c) Destrucción.

En el apartado de destrucción de la información se considera el proceso de borrado seguro.

La información como tal, puede ser recolectada, procesada o almacenada en diversos formatos digitales, como pueden ser dispositivos de almacenamiento fijos o removibles.

Al final del ciclo de vida de la información, se deben emplear mecanismos de destrucción y borrado seguro para evitar que la información quede al alcance de terceros no autorizados.

2. BORRADO SEGURO.

2.1. Métodos No Considerados Válidos para Borrar Datos de Forma Segura.

Dentro de los métodos que no se consideran válidos para llevar a cabo el borrado seguro, son los dispuestos por el propio sistema operativo como con la opción «eliminar» o la tecla «Supr» o «Delete», debido a que esto solo realiza el borrado exclusivamente en la «lista de archivos» sin que se elimine el archivo como tal.

Al formatear un dispositivo normalmente se sobrescribe el área destinada a la «lista de archivos» sin que el área de datos donde se encuentra el contenido de los archivos haya sido alterada.

Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la «lista de archivos» como del contenido del mismo, no se reconocen como métodos válidos para el borrado seguro de la información.

2.2. Métodos Válidos para Realizar el Borrado Seguro.

El Instituto FONACOT empleará y/o hará que se utilicen tecnologías eficaces para evitar completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento, las tecnologías deben hacer uso de cualquiera de las siguientes acciones, desmagnetización, destrucción física y la sobreescritura en la totalidad del área de almacenamiento de la información.

2.2.1. Desmagnetización.

Consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método será válido para la destrucción de datos de los dispositivos magnéticos, como, por ejemplo, los discos duros, cintas magnéticas de backup, etc.

2.2.2. Destrucción Física.

La destrucción física considera la desintegración, pulverización, fusión e incineración.

En el caso de los discos duros se debe asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.2.3. Sobreescritura.

La sobreescritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento, esto se realizará accediendo al contenido de los dispositivos y modificando los valores almacenados.

2.3. Documentación de las Operaciones Realizadas para el Borrado Seguro.

Las herramientas tecnológicas que sean utilizadas por el Instituto FONACOT y/o proveedores que estén relacionados en el borrado seguro, deben generar reportes que permitan avalar el proceso que se ha seguido, detallando quien, que, como, cuando y donde ha sido realizado el borrado seguro.

La herramienta utilizada para el borrado seguro debe generar 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 detallada del medio donde se realizará el borrado.
- 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.

En caso de que el borrado lógico no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte.

2.4. Dispositivos a los que se les Aplica el Borrado Seguro.

Para elementos de infraestructura de servidores y almacenamiento que formen parte de la solución del Instituto FONACOT 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 del servicio 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 al Instituto FONACOT el certificado del borrado seguro.

2.5. Estándares y Certificación de Herramientas Aprobados para el Borrado Seguro.

La herramienta de borrado seguro debe cumplir con al menos uno de los estándares:

- DOD 5220.22-M.
- NAVSO P-5239-26.
- NCSC-TG-025.
- NSA 130-1.
- BRUCE SCHNEIER ´S ALGORITHM.
- HMG INFOSEC STANDARD 5, HIGHER STANDARD.
- NIST 800-88 / ATA SECURE ERASE (+ ASSURANCE).

Y al menos una de las siguientes certificaciones:

- CESG.
- COMMON CRITERIA.
- NSTL.
- OTAN.
- MINISTERIO DE DEFENSA DE LOS ESTADOS UNIDOS.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

25. POLÍTICA DE GESTIÓN DE PARCHES DE SISTEMAS OPERATIVOS.

1. INTRODUCCIÓN.

El Instituto FONACOT consciente de que la delincuencia cibernética ha crecido exponencialmente en la última década, los hackers informáticos cada vez son más creativos y encuentran nuevas formas de explotar las vulnerabilidades. Uno de los puntos de entrada más comunes para estos ataques son los sistemas sin parches. Cada vez que se lanza un parche de seguridad, los atacantes encuentran una nueva vulnerabilidad que se puede explotar (en los sistemas sin parches) y comienzan a explorar para detectar la debilidad.

2. GESTIÓN DE PARCHES DE SISTEMAS OPERATIVOS.

El Instituto FONACOT debe tener instalados los parches de seguridad críticos en todos sus componentes descritos en el alcance de este documento, considerando las capacidades de los aplicativos y plataformas.

Para ello se deben considerar al menos las siguientes acciones:

- Identificación de activos y software: Se debe llevar a cabo la identificación de componentes y el nivel de parches de seguridad aplicados, de manera que los cambios se realicen sin riesgos y en caso de producirse algún problema en la actualización o aplicación de parches de seguridad, se permita volver a un estado previo conocido y funcional.
- Disponibilidad: Se debe tener un inventario actualizado de los componentes, así como revisar el listado de actualizaciones y parches de seguridad disponibles e identificar cuál de ellos afecta a cada componente.
- Aplicabilidad: Los parches de seguridad publicados y actualizaciones se aplican de acuerdo con la criticidad en temas de seguridad que conlleve a cerrar brechas identificadas previamente. Por lo que se debe verificar si el parche de seguridad o actualización son viables.
 - En el caso de los parches de Windows se deben aplicar después del segundo martes de cada mes que publican los parches.
 - Las demás tecnologías se aplican a fin de mes si hubiera parches por aplicar.
- Adquisición: Se deben obtener los archivos de actualización, así como los parches de seguridad de una fuente confiable.
- Validación: Asegurar que la actualización y/o aplicación de parches no impacta de manera negativa la confidencialidad, integridad o disponibilidad de los sistemas de información. Para tal efecto se deben realizar comprobaciones sobre las implicaciones de la actualización o aplicación de parches de seguridad.
- Despliegue: Durante el proceso de validación se debe crear un paquete de despliegue. El paquete debe contener el/los archivo(s) de actualización o parches y las instrucciones de instalación, así como un listado de los componentes en los que realizará el despliegue.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

26. POLÍTICA DE NAVEGACIÓN SEGURA.

1 INTRODUCCIÓN.

Debido a la creciente necesidad de conexión a Internet, esto implica nuevos riesgos que deben ser abordados para salvaguardar los activos de información del Instituto FONACOT.

2 NAVEGACIÓN SEGURA.

2.1. Restricción en la Navegación de la Red.

Se deben utilizar herramientas para bloquear automáticamente sitios web no deseables. Estas herramientas deben instalarse en servidores proxy u otros servidores como firewalls. El fomento de un ambiente de trabajo no hostil debe ser respaldado a través del bloqueo de sitios pornográficos, sitios que apoyan lenguaje prejuicioso, etc.

Se debe restringir:

- El acceso a redes sociales (Facebook, Twitter, YouTube, etc.), así como a servicios de correo electrónico públicos (Hotmail, Yahoo!, Gmail, etc.), aplicaciones chat (WhatsApp, Messenger, etc.) y servicios de almacenamiento en la nube (Google Drive, DropBox, WeTransfer, etc.), se debe hacer el requerimiento a través de una solicitud formal que incluya una justificación detallada y precisa. La solicitud se debe presentar a la SGTIC por la Dirección de la Unidad Administrativa a la que pertenece la persona solicitante. La SGTIC turna la solicitud al RSI para su evaluación y en caso de que el requerimiento no ponga en riesgo la seguridad de la información del Instituto, el RSI otorga su visto bueno.
- El personal laboral del Instituto FONACOT debe restringirse a utilizar el Internet exclusivamente para cuestiones de trabajo.
- Queda estrictamente prohibido la ejecución de aplicaciones proxy por el personal laboral del Instituto FONACOT tales como TOR, Ultrasurf u otro parecido que infrinja la seguridad del Instituto FONACOT. En caso de ejecutar aplicaciones de este tipo sin autorización, será considerado como una violación a la seguridad de manera crítica y el colaborador será acreedor a sanciones que el Instituto FONACOT determine.
- Se debe realizar el monitoreo de la navegación a Internet mediante un reporte mensual que sea entregado al RSI con la finalidad de rastrear anomalías y preservar el buen uso de los recursos.
- Queda prohibida la descarga de material para uso personal.
- Queda estrictamente prohibido el acceso a redes con categorías de contenido adulto y la descarga de cualquier tipo malware.
- Queda prohibido el uso del Internet para fines ilícitos, inmorales, personales o de entretenimiento.
- Queda prohibida la descarga y/o instalación de aplicaciones que no sean previamente autorizadas por el RSI.
- Queda prohibida la instalación o ejecución en cualquier punto de la red informática (ordenadores o software) programas o ficheros que deterioren o incrementen el exceso de carga en cualquier punto de esta, perjudicando el rendimiento de la red.
- Queda estrictamente prohibida la instalación o ejecución de cualquier programa o fichero que trate de descubrir información en cualquier elemento de la red, sniffer, escaneo de puertos, etc.

2.2. Segregación de Redes.

Los segmentos de la red deben separarse lógicamente para garantizar la separación de funciones incompatibles y los privilegios de acceso.

Considerando las políticas de control de acceso, los requerimientos de acceso y la evaluación de riesgos, la red debe dividirse en dominios o segmentos apropiados. Estos incluyen al menos los siguientes:

- Desarrollo.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01 Vigencia: Julio, 2024	
--	--	--	---

- Testing.
- Operación.
- Red perimetral.

2.3. Red para Externos.

Se debe contar con redes externas para el personal laboral o proveedores de servicio que requieran internet. El uso de internet dentro del Instituto FONACOT debe ser únicamente para fines laborales y/o de consulta, esta puede ser monitoreada con fines de seguridad.

Las redes designadas al personal externo no deben estar comunicadas con los servicios, aplicativos, bases de datos, equipo, red compartida, repositorio, dispositivos o ningún otro tipo de activo del Instituto FONACOT.

Se debe bloquear automáticamente sitios Web no deseables en la red dedicada para externos, esto incluye el bloqueo de sitios pornográficos, sitios que apoyan lenguaje prejuicioso, etc.

El acceso de proveedores a la red del Instituto FONACOT debe seguir los siguientes puntos:

- El personal externo debe solicitar el ingreso a la red de invitados mediante un portal.
- La solicitud a la red debe contener el nombre del solicitante, nombre del personal laboral del Instituto FONACOT y correo electrónico.
- El personal externo debe aceptar las políticas de acceso a la red local de invitados, antes de conectarse a la red.
- La solicitud debe ser validada por un encargado de la red del Instituto FONACOT.
- Las credenciales de inicio de sesión de los invitados deben caducar después de un período definido.

De requerirse accesos especiales a la red por personal externo, el responsable del Servicio debe ser el encargado de solicitar el acceso a una red que permita la conexión solicitada, al encargado de la red del Instituto FONACOT.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

27. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE SISTEMAS OPERATIVOS.

1. INTRODUCCIÓN.

El Instituto FONACOT depende de servidores, estos equipos son necesarios para entregar datos de forma segura y confiable. Bajo este enfoque se debe garantizar que los servidores mantengan la integridad, la confidencialidad y la disponibilidad de los datos.

2. SEGURIDAD DE LA INFORMACIÓN DE SISTEMAS OPERATIVOS.

El Instituto FONACOT debe identificar todos los servidores asociados dentro del alcance del MGSÍ.

Ningún servidor debe prestar servicios ni formar parte de ningún ambiente (desarrollo, pruebas, calidad, producción) hasta que la DTI y la DIT declaren que la configuración del sistema operativo es segura, bajo este orden ningún servidor debe estar conectado a la red del Instituto FONACOT, se demuestre que la configuración sea segura.

El RSI solicitará periódicamente las configuraciones de seguridad del sistema operativo, el cual tomará las acciones que correspondan.

2.1 Generales.

- La instalación del sistema operativo debe realizarse desde una fuente aprobada.
- La aplicación de parches debe ser proporcionados por el proveedor y realizarse conforme a la política de gestión de parches de sistemas operativos.
- Se debe realizar la eliminación de software, servicios del sistema y controladores innecesarios.
- Se deben establecer los parámetros de seguridad, protecciones de datos, archivos y habilitar el registro de auditoría.
- Se debe deshabilitar o cambiar la contraseña de cuentas predeterminadas.
- La DIT, DTI y el RSI, supervisan los problemas de seguridad, tanto internos como externos al Instituto FONACOT y en su caso gestionan la publicación de parches de seguridad.
- La SGTIC probará los parches de seguridad antes de su instalación, por lo que debe tener la capacidad de disponer de los recursos necesarios.
- Los parches de seguridad deben implementarse dentro del plazo especificado en la política de gestión de parches de sistemas operativos.

2.2 Específicos.

El Instituto FONACOT y sus proveedores de servicio deben tomar como base las guías de configuración de seguridad (Benchmark) publicadas por el Center for Internet Security, Inc. (CIS).

Estas guías establecen los lineamientos de configuración segura para los sistemas operativos y bases de datos.

Para consultar u obtener su última versión, visitar <http://benchmarks.cisecurity.org>.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

28. POLÍTICA DE GESTIÓN DE INCIDENTES CIBERNÉTICOS.

1. INTRODUCCIÓN.

Derivado del creciente número de ataques cibernéticos en el país, el Instituto FONACOT desarrolla esta política de gestión de incidentes cibernéticos para establecer los mecanismos que se deben usar ante los incidentes cibernéticos que se presenten en los activos esenciales del Instituto FONACOT.

2. GESTIÓN DE INCIDENTES CIBERNÉTICOS.

- El Instituto FONACOT, opera cabalmente el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos de la Guardia Nacional.
- El Instituto FONACOT, debe conformar y establecer el grupo ERISC.
- El grupo ERISC debe considerar al menos los roles y responsabilidades establecidos en el Anexo 1 del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.
- El Instituto FONACOT, debe establecer y actualizar una base de datos de contactos para la identificación de los responsables del ERISC y del RSI.
- El Instituto FONACOT, debe identificar los activos esenciales de información, los cuales deben contar con la siguiente información:
 - Site – KIO.
 - Origen.
 - Unidad de procesamiento.
 - Estatus.
 - Hostname.
 - Aplicación.
 - Nube.
 - Descripción.
 - Plataforma.
 - Ubicación física.
 - Máscara de subred.
 - Gateway.
 - VLAN ID.
 - Ambiente.
 - IP Producción.
 - IP backup / mgt.
 - IP Pública.
 - Marca / Modelo.
 - Número de serie.
 - Hardware físico / virtual.
 - Sistema Operativo.
- El Instituto FONACOT, debe determinar el nivel de implementación actual de la seguridad de la información actual, con base en el cuestionario metodológico del Anexo 4 del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.
- El Instituto FONACOT debe recibir alertas y boletines de vulnerabilidades y amenazas cibernéticas del CERT-MX previa suscripción, en caso de presentarse cambios en los datos de contacto del RSI, estos deben ser informados al correo cert-mx@sspc.gob.mx.
- En caso de presentarse algún incidente cibernético que sea clasificado de nivel crítico, muy alto o alto, de acuerdo con el Anexo 8 del Protocolo Nacional Homologado de Gestión de Incidentes, se debe reportar a las siguientes autoridades.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Autoridad	Datos de contacto
Guardia Nacional:	phishing@gn.gob.mx
Policía Cibernética:	policia.cibernetica@ssc.cdmx.gob.mx
CERT-MX:	cert-mx@sspc.gob.mx o a través de la página web https://www.gob.mx/gncertmx

- El reporte debe contener al menos la siguiente información:
 - Destinatario.
 - Datos del remitente.
 - Nombre de la Institución.
 - Asunto.
 - Descripción del incidente.
 - Evidencia.

- El Instituto FONACOT está al pendiente de la Semaforización del protocolo respecto al entorno de amenazas y riesgos, que emite el CERT-MX a través de sus medios digitales.
- El Instituto FONACOT realiza el monitoreo proactivo y reactivo a sus activos esenciales.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

29. POLÍTICA DE SOLICITUD DE DESBLOQUEO DE CUENTA Y REINICIO DE CONTRASEÑA.

1. INTRODUCCIÓN.

El tratamiento diario de la información del Instituto FONACOT requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales se utilizan cuentas de acceso y contraseñas.

Las cuentas pueden ser bloqueadas y en el caso de las contraseñas estas pueden ser revocadas debido a alguna de las siguientes circunstancias:

1. Que el empleado sea dado de baja del Instituto FONACOT.
2. Contraseña comprometida debido a la pérdida de la confidencialidad.
3. Error mecánico y/o humano al momento de digitar la contraseña y agotar el número de oportunidades para ingresar la contraseña correcta.
4. Olvido de la contraseña.

2. SOLICITUD DE DESBLOQUEO DE CUENTA Y REINICIO DE CONTRASEÑA.

Solicitud de desbloqueo de cuenta y reinicio de contraseña.

- El personal debe levantar un ticket de servicio ante la Mesa de Servicio del Instituto FONACOT, solicitando el desbloqueo de su cuenta y reinicio de contraseña.
- El personal debe proporcionar a la Mesa de Servicio información adicional para que se documente la solicitud de desbloqueo de cuenta y reinicio de contraseña por parte de la Mesa de Servicio, esta información debe ser:
 - Motivo por el que se desbloquea la cuenta y genera la contraseña temporal de un solo uso.
 - Posibles observaciones, incidentes, olvido, otros.


Creación y entrega de contraseña temporal de un solo uso.

La Mesa de Servicio realiza lo siguiente:

- Documenta la creación de la contraseña temporal de un solo uso.
 - Fecha de creación de la contraseña.
 - Responsable de la custodia.
 - Periodo de validez.
- La contraseña temporal de un solo uso debe cumplir con los lineamientos establecidos en el Procedimiento de contraseñas descrito en este MGSI.
- En caso de ser necesario se restablecerá el múltiple factor de autenticación.
- Proporciona a la persona solicitante la contraseña temporal de un solo uso, esto se realiza a través del correo electrónico institucional o a través de llamada telefónica.

Uso y cambio de la contraseña temporal de un solo uso.

En el primer inicio de sesión usando la contraseña temporal de un solo uso, la persona solicitante debe cambiarla por otra que sea creada por él. En la creación de la nueva contraseña, se deben cumplir los lineamientos establecidos en el Procedimiento de contraseñas descrito en este MGSI.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

30. POLÍTICA DE EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS TECNOLÓGICOS.

1. INTRODUCCIÓN.

El Instituto FONACOT reconoce la importancia de preservar los activos tecnológicos, por lo que debe realizar una gestión de riesgos tecnológicos a través de la identificación, evaluación y tratamiento de los riesgos tecnológicos.

El objetivo de esta Política es establecer los criterios básicos necesarios para la gestión de riesgos tecnológicos del Instituto FONACOT.

2. EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS TECNOLÓGICOS.

Se consideran todos los activos tecnológicos de información del Instituto FONACOT, incluso aquellos provistos y/o gestionados mediante contratos con terceros.

El Instituto FONACOT debe:

- Establecer, formalizar y poner en práctica la metodología para la gestión de riesgos que está definida en el MGSi.
- En el caso de que sea necesario realizar una evaluación de riesgos a través del uso de metodologías y/o herramientas pertenecientes a otra instancia del gobierno federal, la información con la que se debe alimentar a dicha herramienta debe coincidir con la que es utilizada en el proceso de evaluación de riesgos indicado en el MGSi.
- Definir y establecer en forma explícita el nivel de aceptación del riesgo tecnológico.
- Contar con la aprobación explícita de los planes de tratamiento del riesgo residual que se deriven del resultado de cada evaluación de riesgos.
- Realizar evaluaciones semestrales del riesgo tecnológico.
- Mantener informadas a las partes involucradas y reguladores sobre el estado del riesgo tecnológico.

El RSI debe velar por el cumplimiento de la presente política y brindar asesoramiento en la identificación de las amenazas y las vulnerabilidades que pueden afectar a los activos tecnológicos, debe informar sobre los resultados de las evaluaciones de los riesgos tecnológicos. En conjunto con los responsables de los activos de información determinan las acciones de tratamiento de los riesgos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

31. PROCEDIMIENTO ACCIONES CORRECTIVAS Y OPORTUNIDADES DE MEJORA.

1. INTRODUCCIÓN.

El propósito del MGSÍ es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en dichos riesgos, el entorno y las tecnologías.

A través del ciclo de mejora continua del MGSÍ se identifica la oportunidad de mejorar la seguridad efectiva de la información relacionada con sus procesos, que le permita mantener niveles óptimos con relación a la confidencialidad, integridad y disponibilidad de la información.

De lo anterior se deriva la necesidad de contar con un procedimiento para llevar a cabo las acciones correctivas y oportunidades de mejora.

2. ACCIONES CORRECTIVAS Y OPORTUNIDADES DE MEJORA.

El RSI asegura la correcta documentación de las acciones correctivas y de las oportunidades de mejora, así como el seguimiento hasta su solución, validando el cierre del hallazgo y la efectividad de las acciones.

El responsable del plan de acción debe asegurar su cumplimiento, cierre de la observación o hallazgo en tiempo y forma.

El responsable asignado para la solución de la acción y/o aplicación de la mejora debe coordinar y asignar al equipo las responsabilidades y las actividades necesarias para el análisis y solución del problema o situación de mejora.

El equipo de trabajo debe analizar y resolver el problema o situación de mejora de acuerdo con las actividades asignadas por el responsable del equipo.

3. DESARROLLO.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
Responsable del Hallazgo u Observación	<ol style="list-style-type: none"> 1. Detecta la necesidad de implantar Acciones Correctivas u Oportunidades de Mejora que puede surgir por la detección de: <ol style="list-style-type: none"> a. Una No Conformidad. b. Una Observación. <p>Las no conformidades pueden detectarse en:</p> <ol style="list-style-type: none"> a. Quejas y/o sugerencias del personal. b. Desviaciones en el proceso. c. Fallas en el MGSÍ. d. Resultados de Auditorías Internas y Externas. e. Registros, estadísticas, tendencias, reportes de desempeño (cuando estos no sean favorables y se considere necesaria su aplicación). 	Quejas y/o Sugerencias del personal. Documentación de Desviaciones en el Proceso Resultados de Auditorías Internas y Externas Registros, Estadísticas, Tendencias, Reportes de Desempeño (cuando estos no sean favorables y se considere necesaria su aplicación)
Responsable del Hallazgo u Oportunidad de Mejora	<ol style="list-style-type: none"> 2. Elabora Solicitud de Acción u Oportunidad de Mejora en conjunto con el RSI. 	Solicitud de Acción u Oportunidad de Mejora
Responsable del Hallazgo u Oportunidad de Mejora	<ol style="list-style-type: none"> 3. Forma un equipo de trabajo con los responsables de las áreas involucradas (cuando aplique) y llevan a cabo el análisis con los involucrados, considerando lo siguiente: 	Solicitud de Acción u Oportunidad de Mejora. Análisis Causa Raíz. Plan de Trabajo



	<p>a. Tienen un máximo 5 días hábiles para realizar el análisis y definir la causa raíz, la cual será identificada mediante una lluvia de ideas entre el responsable del área involucrada y el personal laboral responsable de la No conformidad, determinar las acciones a tomar (correcciones y acciones correctivas) y entregarla al responsable del Sistema de Gestión.</p> <p>El análisis realizado por los involucrados, así como los resultados obtenidos, son registrados en la Solicitud de Acción u Oportunidad de Mejora, determinando así el plan de trabajo a seguir, según la magnitud o impacto de la No Conformidad u Observación.</p>	
Responsable del Hallazgo u Oportunidad de Mejora	4. Implanta y da seguimiento a las acciones en tiempo y forma.	Plan de Trabajo
RSI	<p>5. Da seguimiento a cada Solicitud de Acción u Oportunidad de Mejora, registrando en la parte posterior del formato la fecha, observaciones y su firma, así como recabando la firma del responsable de la No Conformidad.</p> <p><i>En caso de no evidenciarse un avance y cumplimiento a las fechas de término planeadas, solicita la justificación por escrito de las mismas y en caso de presentarse por segunda ocasión notifica a la Dirección de la Unidad Administrativa inmediata.</i></p>	Plan de Trabajo Solicitud de Acción u Oportunidad de Mejora.
RSI	6. Concentra todas las Solicitudes de Acción u Oportunidades de Mejora en su archivo de seguimiento y actualiza el porcentaje de avance de cada una.	Plan de Trabajo Solicitud de Acción u Oportunidad de Mejora.
RSI	7. Evalúa que las acciones que se reportan como terminadas hayan sido efectivas para evitar la recurrencia.	Plan de Trabajo Solicitud de Acción u Oportunidad de Mejora.
RSI	8. Analiza y retroalimenta al responsable del Hallazgo u Oportunidad de Mejora en caso de que la No Conformidad u observación no haya sido eliminada.	Plan de Trabajo Solicitud de Acción u Oportunidad de Mejora.
TERMINA PROCEDIMIENTO.		

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

32. PROCEDIMIENTO PARA HABILITAR/DESHABILITAR EL USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPOS DE CÓMPUTO.

1. INTRODUCCIÓN.

Como parte del MGSJ el Instituto FONACOT cuenta con una Política de Uso de Medios de Almacenamiento Externos en Equipos de Cómputo.

De lo anterior se deriva la necesidad de contar con un procedimiento específico para el bloqueo y desbloqueo de puertos USB de los equipos del Instituto FONACOT, este procedimiento tiene la finalidad de minimizar el riesgo relacionado con la extracción no autorizada de información.

Establecer el procedimiento para el bloqueo y desbloqueo de puertos USB de los equipos de cómputo del Instituto FONACOT que son utilizados para la realización de sus actividades laborales, con la intención de que sea restringido el uso de cualquier medio de almacenamiento extraíble que tenga la capacidad de guardar información.

2. USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPOS DE CÓMPUTO.

- La aprobación de las solicitudes para la habilitación de puertos USB de los equipos de cómputo del Instituto FONACOT, corresponde a cada Dirección a la que pertenece el área usuaria de la que proviene cada una de las solicitudes.
- Cada Subdirección General del área usuaria solicitante debe solicitar mediante oficio a la DIT el cambio de estatus sobre los puertos USB (bloqueo / desbloqueo).
- La DIT debe ejecutar las siguientes tareas:
 - Previo a la entrega o reasignación de un equipo de cómputo al personal laboral del Instituto FONACOT, habilitar política de dominio que deshabilita las unidades de CD/DVD, ranuras de memoria externa y puertos USB de un equipo de cómputo.
 - Derivado de una solicitud de alguna Subdirección General hacia la DIT, activar o desactivar la política de dominio que deshabilita las unidades de CD/DVD, ranuras de memoria externa y puertos USB de un equipo de cómputo.
 - Mantener un registro del personal a los que alguna Subdirección General ha solicitado se le desactive el uso de medios de almacenamiento extraíbles en un equipo de cómputo.

3. DESARROLLO.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
Dirección de la Unidad Administrativa	1. Envía la solicitud para habilitar el uso de medios de almacenamiento extraíbles.	Solicitud
Dirección de la Unidad Administrativa	2. Recopila la información requerida para la solicitud hacia la Subdirección General correspondiente: <ul style="list-style-type: none"> a. Personal con nivel mando medio o superior. b. Puesto. c. Área o departamento. d. No. Extensión. e. Correo electrónico. f. Número de serie del equipo de cómputo. g. Nombre de la persona quien tiene asignado el equipo involucrado. h. Justificación que sustenta la petición. 	Solicitud
Dirección de la Unidad Administrativa	3. Envía solicitud a la Subdirección General correspondiente.	Solicitud

Subdirección General correspondiente	4. Recibe solicitud por parte de la Dirección de la Unidad Administrativa correspondiente.	Solicitud
Subdirección General correspondiente	5. Válida a solicitud: a. Que la información de la solicitud esté completa. b. Que la justificación para habilitar el uso de medios de almacenamiento extraíbles sea válida.	Solicitud
Subdirección General correspondiente	6. Firma de autorización la solicitud para la apertura de puertos USB.	Solicitud
Subdirección General correspondiente	7. Envía la solicitud autorizada a la DIT a través de oficio.	Solicitud
DIT	8. Recibe las solicitudes de las diferentes Subdirecciones Generales para habilitar/deshabilitar el uso de medios de almacenamiento extraíbles en un equipo de cómputo.	Solicitud
DIT	9. Ejecuta los cambios solicitados a través del proveedor correspondiente.	Solicitud
DIT	10. Coordina las acciones para que el proveedor encargado de realizar las configuraciones de la política mantenga actualizada la bitácora del personal a los que se les active el uso de medios de almacenamiento extraíbles en un equipo de cómputo.	Solicitud
DIT	11. Válida que los entregables mensuales del proveedor correspondiente se integre el estado que guarda la bitácora del personal que tienen activo el uso de medios de almacenamiento extraíbles en un equipo de cómputo.	Bitácora del personal
DIT	12. Envía la notificación a la Subdirección General correspondiente, una vez que se confirma que las acciones solicitadas fueron ejecutadas.	Solicitud
TERMINA PROCEDIMIENTO.		

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

33. PROCEDIMIENTO DE GESTIÓN DE CUENTAS.

1. INTRODUCCIÓN.

El MCSI requiere que exista un ambiente de control de seguridad de la información sobre la gestión de cuentas privilegiadas y no privilegiadas (enunciativo más no limitativo a lectura, de sistema, de escritura, de eliminación, etc.).

2. GESTIÓN DE CUENTAS.

- Únicamente el personal laboral autorizado por la SGTIC puede realizar la solicitud de cuentas privilegiadas y no privilegiadas para un proveedor de servicio.
- Toda la administración de cuentas privilegiadas o no privilegiadas que se requiera debe estar documentada mediante el formato "Solicitud de Cuenta".
- Los proveedores deben integrar un informe mensual donde se mencionen las acciones realizadas con el uso de la cuenta.
- El acceso a las cuentas privilegiadas y no privilegiadas de los proveedores deben ser a través de una herramienta de PAM.
- El acceso a las cuentas privilegiadas y no privilegiadas del Instituto FONACOT deben ser a través de una herramienta de PAM, de lo contrario se debe justificar mediante oficio por la Dirección requirente, este requerimiento debe ser dirigido al RSI para su revisión y aprobación.

3. DESARROLLO.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
Solicitante	1. Elabora correo electrónico con la solicitud autorizada por la Dirección de la Unidad Administrativa para gestionar los privilegios sobre las cuentas privilegiadas, cuentas de servicio o cuentas de aplicativos.	Formato de Solicitud de Cuenta.
Solicitante	2. Recopila la información requerida para la solicitud, el formato Solicitud de Cuenta: <ul style="list-style-type: none"> a. Nombre del solicitante. b. Puesto del solicitante. c. Unidad Administrativa. d. Nombre del sistema (Servidor, aplicativo, sistema operativo) involucrado. e. Nombre del dominio. f. Cuenta interna o externa. g. Comando por ejecutar. h. Ruta de ejecución. i. Periodo de vigencia. j. Justificación del por qué se otorga el acceso. k. Nombre del proveedor que tiene asignado el sistema involucrado. l. Privilegios requeridos para la cuenta. m. Periodo de vigencia de contraseña (si aplica). 	Formato de Solicitud de Cuenta
Solicitante	3. Envía la solicitud a través del correo electrónico al RSI.	Formato de Solicitud de Cuenta.
RSI	4. Recibe y valida la información del formato y determina si procede su aprobación.	Formato de Solicitud de Cuenta.
RSI	5. Válida lo siguiente: <ul style="list-style-type: none"> a. Que la información de la solicitud esté completa. 	Formato de Solicitud de Cuenta.



	b. Que la justificación para la modificación de la cuenta privilegiada sea válida y tenga fundamento sustentable.	
RSI	6. Analiza el riesgo de la solicitud.	Formato de Solicitud de Cuenta.
RSI	<i>Si del análisis de riesgo de la solicitud, se determina que genera un riesgo de seguridad, continúa con actividad 7.</i> 7. Rechaza la solicitud.	Formato de Solicitud de Cuenta.
RSI	<i>Si del análisis de riesgo de la solicitud, no se determina ningún riesgo, continúa con actividad 8.</i> 8. Aprueba la solicitud.	Formato de Solicitud de Cuenta.
Proveedor Responsable del PAM	9. Recibe correo electrónico con la solicitud por parte del RSI.	Formato de Solicitud de Cuenta.
Proveedor Responsable del PAM	10. Realiza la acción determinada en la solicitud: a. Creación: Crea la cuenta privilegiada o no privilegiada. b. Asignación: Identifica la cuenta privilegiada o no privilegiada y la asigna al solicitante con los privilegios correspondientes. c. Modificación: Identifica la cuenta privilegiada o no privilegiada y modifica lo solicitado (nombre, privilegios). d. Eliminación: Identifica la cuenta privilegiada o no privilegiada y realiza la suspensión y/o eliminación.	Formato de Solicitud de Cuenta.
Proveedor Responsable del PAM	11. Documenta la acción realizada con los siguientes datos: a. Responsable de la acción en la cuenta privilegiada. b. Cuenta privilegiada. c. Contraseña cifrada (en caso de creación/asignación). d. Ubicación de la cuenta (en caso de creación/asignación). e. Privilegios de la cuenta (en caso de creación/asignación/modificación). f. Evidencia de la eliminación de la cuenta (en caso de eliminación).	Formato de Solicitud de Cuenta.
Proveedor Responsable del PAM	12. Envía correo electrónico con la documentación de la acción realizada solicitante y al RSI.	Formato de Solicitud de Cuenta.
Solicitante	13. Recibe correo electrónico con los datos solicitados.	Formato de Solicitud de Cuenta.
Solicitante	14. Intenta realizar la acción solicitada con la cuenta privilegiada o no privilegiada.	Formato de Solicitud de Cuenta.
Solicitante	<i>Si la actividad 14 se cumple continúa con actividad 15.</i> 15. Envía respuesta por correo electrónico al Proveedor Responsable del PAM y al RSI, indicando la confirmación.	Formato de Solicitud de Cuenta.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Personal del Instituto FONACOT Solicitante	Si la actividad 14 no se cumple, continúa con actividad 4. 16. Envía correo al Proveedor Responsable del PAM y al RSI y regresar a la actividad 2, para que la solicitud sea realizada nuevamente.	Formato de Solicitud de Cuenta.
TERMINA PROCEDIMIENTO.		

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

34. PROCEDIMIENTO DE CONTRASEÑAS.

1. INTRODUCCIÓN.

El propósito de este procedimiento es establecer un estándar para la creación y mantenimiento de contraseñas en el Instituto FONACOT que son utilizadas por el personal para la realización de sus actividades laborales, con la intención de mantener la confidencialidad de la información evitando el acceso no autorizado de la información en los sistemas aplicativos que accedan a estos activos.

2. CONTRASEÑAS.

Creación de Contraseña.

- Todas las contraseñas deben cumplir con las pautas de construcción de contraseñas.
- Se deben usar contraseñas únicas y exclusivas para cada una de las cuentas asignadas.
- No se deben usar las contraseñas empleadas en el Instituto FONACOT en cuentas personales.
- Las cuentas que tienen privilegios de alto nivel otorgados a través de grupos o programas como "sudo" deben tener una contraseña única de todas las otras cuentas. Además, se recomienda utilizar alguna forma de autenticación multifactorial para cualquier cuenta privilegiada.

Pautas de Construcción de Contraseñas.

- La contraseña debe tener al menos 8 caracteres.
- La contraseña debe contener letras mayúsculas y minúsculas, números y caracteres especiales.
- La contraseña debe cambiar cada 2 meses.
- No debe incluir nombres propios.
- No se debe repetir la misma contraseña que se haya utilizado anteriormente.
- No debe incluir números consecutivos o más de dos números iguales.
- Contraseña de un solo uso para el primer inicio sesión.

Cambio de Contraseña.

- Cambio obligatorio después del primer ingreso o cambio de contraseña.
- Las contraseñas deben cambiarse solo cuando existan razones para creer que una contraseña se ha visto comprometida.
- El descifrado o adivinación de contraseñas puede ser realizado de forma periódica o aleatoria. Si se adivina o se descifra una contraseña durante uno de estos escaneos, el personal debe cambiarla para cumplir con las pautas de construcción de contraseña.

Protección con Contraseña.

- Las contraseñas no deben compartirse con nadie, incluidos supervisores y compañeros de trabajo.
- Todas las contraseñas deben tratarse como información confidencial del Instituto FONACOT.
- Las contraseñas no deben insertarse en mensajes de correo electrónico, ni revelarse por teléfono a nadie.
- Las contraseñas solo se pueden almacenar en "administradores de contraseñas" autorizados por el Instituto FONACOT.
- No utilice la función "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).
- Bajo la sospecha de tener contraseñas comprometidas, se debe informar a la mesa de servicio (*111) y realizar el cambio de todas las contraseñas.
- Directrices de contraseñas en desarrollo seguro de aplicaciones localizadas en la política de desarrollo seguro.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

35. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

La respuesta a incidentes de seguridad de la información es un componente crítico en la operación del Instituto FONACOT en donde es indispensable reducir el impacto de incidentes a través de la mitigación y remediación de manera integral y en el menor tiempo posible.

La política de respuesta a incidentes de seguridad de la información proporciona los lineamientos para que los equipos de tecnología y del negocio integren esfuerzos, considerando información de contacto de los participantes, matrices de escalamiento, acuerdos de niveles de servicio (SLA), clasificación de severidad e impacto, así como, plazos de mitigación y remediación.

Establecer una política que contemple la respuesta a incidentes de seguridad de la información en el Instituto FONACOT, puntualmente los incidentes que se deriven por errores, fallos no intencionados, ataques intencionados y ataques a proveedores de servicios críticos.

2. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El ERISC del Instituto FONACOT se rige bajo las reglas de operación de dicho Manual.

El Instituto FONACOT implementa y mantiene actualizado un modelo para la respuesta a incidencias de seguridad de la información en entornos productivos, bajo las siguientes fases:

A. Preparación.

A1. Actividades preliminares.

A1.1 Comunicación e instalaciones para la respuesta de incidentes.

A1.2 Equipo requerido para el análisis de incidentes.

A1.3 Recursos para el análisis de incidentes.

A2. Prevención de incidentes.

A2.1 Evaluación de riesgos.

A2.2 Seguridad de servidores.

A2.3 Seguridad de red.

A2.4 Prevención de malware.

A2.5 Conciencia y capacitación.

B. Detección.

B1. Detección de eventos relacionados con incidentes de seguridad.

B1.1 Identificación de incidentes.

B2. Priorización del manejo del incidente.

B3. Informar el incidente al personal laboral y externos.

C. Respuesta y recuperación

C1. Contención del incidente.

C2. Adquisición, preservación, aseguramiento y documentación de evidencia.

C3. Erradicación y recuperación del incidente.

C4. Lecciones aprendidas.

C5. Uso de datos de incidentes recopilados.

D. Actualización y Mejora Continua Institucional.

D1. Implementación de un MGSI.

D2. Implementación de herramientas de monitoreo y detección de incidentes.

D3. Capacitación especializada continua a los equipos de respuesta.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

A. Preparación.

A1. Actividades Preliminares.

A1.1 Comunicación e instalaciones para la respuesta de incidentes.

El ERISC del Instituto FONACOT realizará lo siguiente:

- Mantiene actualizada la información de contacto a los integrantes de los equipos internos de respuesta a incidentes y otros contactos fuera del Instituto FONACOT, como la policía cibernética; la información debe incluir números de teléfono, direcciones de correo electrónico, claves de cifrado públicas e instrucciones para verificar la identidad del contacto.
- Mantiene actualizada la información de las guardias de cada una de las áreas de la SSOS y niveles de servicio necesarios para mitigar incidencias productivas.
- Mantener actualizada la información respecto a los mecanismos de notificación de incidentes, números de teléfono, direcciones de correo electrónico, formularios en línea y sistemas seguros de mensajería instantánea que el personal puede usar para informar incidentes sospechosos; en donde al menos un canal de comunicación debería permitir al personal informar incidentes de forma anónima para reportar incidentes de seguridad.

La SGTIC y el RSI realizará lo siguiente:

- Utilizará un sistema de seguimiento de problemas para rastrear información del estado que guardan los incidentes.
- Proveerá a los miembros del equipo ERISC y personal laboral de guardia de otras áreas de la SSOS de teléfonos inteligentes para proporcionar coordinación y asistencia fuera del horario laboral.
- Proveerá software de cifrado que se utilizará para las comunicaciones entre los miembros del equipo de respuesta a incidentes, dentro del Instituto FONACOT y agencias federales, el software debe usar un algoritmo de cifrado.
- El Instituto FONACOT proveerá de una locación física segura (Sala de guerra) para comunicación central y coordinación en caso de incidencias de alto impacto.
- El Instituto FONACOT proveerá de una locación física segura para el almacenamiento de evidencia y otros materiales sensibles resultantes de la respuesta a incidentes de seguridad.
- Adicionar información de relacionada con la cadena de custodia y custodios de la información relacionada con incidentes.

A1.2 Equipo requerido para el análisis de incidentes.

El Instituto FONACOT proveerá de equipo, herramientas y otro material de apoyo que sea necesario para la respuesta a incidentes, al respecto se lista lo siguiente de manera no limitativa:

- Estaciones de trabajo forenses y/o dispositivos de respaldo para crear imágenes de disco, preservar archivos de registro y guardar otros datos de incidentes relevantes.
- Computadoras portátiles para actividades como el análisis de datos, el rastreo de paquetes y la redacción de informes.
- Estaciones de trabajo, servidores y equipos de red de repuesto, o los equivalentes virtualizados, que pueden usarse para muchos propósitos, como restaurar copias de seguridad y probar malware.
- Medios de almacenamiento extraíbles en blanco.
- Impresora portátil para imprimir copias de archivos de registro y otra evidencia de sistemas no conectados en red.
- Sniffers de paquetes y analizadores de protocolos para capturar y analizar el tráfico de red.
- Software forense digital para analizar imágenes de disco.
- Medios extraíbles con versiones confiables de programas que se utilizan para recopilar evidencia de los sistemas.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Accesorios para la recopilación de pruebas, incluidos cámaras digitales, grabadoras de audio, formularios de cadena de custodia, bolsas y etiquetas de almacenamiento de pruebas, cinta adhesiva para sellado de elementos de pruebas, todo lo anterior con la finalidad de preservar la evidencia para posibles acciones legales.

A1.3 Recursos para el análisis de incidentes.

- Listas de puertos, incluidos los puertos de uso común y los puertos de troyanos.
- Documentación para sistemas operativos, aplicaciones, protocolos y detección de intrusos y productos antivirus.
- Diagramas de red y listas de activos críticos, como servidores de bases de datos.
- Líneas base actuales de la actividad esperada de la red, el sistema y la aplicación.
- Hashes criptográficos de archivos críticos para acelerar el análisis de incidentes, verificación y erradicación.

A2. Prevención de Incidentes.

A2.1 Evaluación de riesgos.

Los riesgos deben ser evaluados regularmente conforme a la metodología de evaluación de riesgos del Instituto FONACOT.

A2.2 Seguridad de servidores.

Todos los servidores del Instituto FONACOT deben ser reforzados (hardening) usando configuraciones personalizadas. Mantener cada servidor correctamente actualizado, los servidores deben configurarse para seguir el principio del mínimo privilegio, otorgar al personal sólo los privilegios necesarios para realizar tareas autorizadas. Los servidores deben tener habilitada la auditoría para registrar eventos importantes relacionados con la seguridad. La seguridad de los servidores y sus configuraciones deben monitorearse continuamente, buscando posibles precursores o indicadores de incidentes.

A2.3 Seguridad de red.

El perímetro de la red debe configurarse para negar toda actividad que no esté expresamente permitida. Esto incluye asegurar todos los puntos de conexión, como redes privadas virtuales (VPN), puntos de acceso a redes inalámbricas y conexiones dedicadas a enlaces con otras dependencias federales y/o financieras privadas. Lo anterior conforme a la Política de seguridad en las comunicaciones y la Política de conexiones VPN (Red Privada Virtual) Cliente – Servidor.

A2.4 Prevención de malware.

El software para detectar y detener el malware debe implementarse en todo el Instituto FONACOT. La protección contra malware debe implementarse a nivel de servidor (por ejemplo, sistemas operativos de servidores y estaciones de trabajo), el nivel de servidor de aplicaciones (por ejemplo, servidor de correo electrónico, servidores proxy web) y el nivel de cliente de aplicaciones (ejemplo, clientes de correo electrónico, clientes de mensajería instantánea). Lo anterior conforme a la Política de Protección Contra Malware.

A2.5 Conciencia y capacitación.

El personal debe conocer las políticas y los procedimientos con respecto al uso apropiado de redes, sistemas y aplicaciones. Las lecciones aprendidas aplicables de incidentes anteriores también deben compartirse con el personal para que puedan ver cómo sus acciones podrían afectar al Instituto FONACOT. Mejorar la conciencia del personal respecto con los incidentes debería reducir la frecuencia de los incidentes. El personal de TI debe estar capacitado para que puedan mantener sus redes, sistemas y aplicaciones de acuerdo con los estándares de seguridad del Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

B. Detección.

B1. Detección de Eventos Relacionados con Incidentes de Seguridad.

Los eventos que pueden afectar la operación normal del Instituto FONACOT bajo el contexto de seguridad de la información son los siguientes:

Evento 1: Ataques a proveedores de servicios críticos.

Este evento tiene relación con los servicios críticos provistos por un tercero y que, en caso de falla parcial o total, las operaciones del Instituto FONACOT pueden verse afectadas de manera indirecta.

Se considera la pérdida de servicios provistos al Instituto FONACOT por parte de los proveedores de servicios críticos, tales como servicios de procesamiento de datos, infraestructura pública y de comunicaciones. Este evento tiene un enfoque de variables externas.

Evento 2: Errores y fallos no intencionados.

Este evento tiene relación con fallas en la integridad, confidencialidad y disponibilidad de la información de manera parcial o total, generado por errores y fallos no intencionados en la administración de recursos informáticos, así como en los procesos de la misma gestión de operaciones tecnológicas. Este evento tiene un enfoque de variables internas.

Evento 3: Ataques intencionados.

Este evento tiene relación con fallas en la integridad, confidencialidad y disponibilidad de la información de manera parcial o total, generado por ataques intencionados a los activos informáticos del Instituto FONACOT. Este evento tiene un enfoque tanto de variables internas como de variables externas.

B1.1 Identificación de incidentes.

Los signos de un incidente se clasifican como:

1. Precursores – Señal de que puede ocurrir un incidente en un futuro.
2. Indicadores – Señal de un incidente que puede haber ocurrido o está ocurriendo ahora.

Fuentes de precursores e indicadores:

- Alertas de herramientas de seguridad.
- Registros de sistema operativo, servicios y aplicaciones.
- Registros de dispositivos de red.
- Flujos en la red.
- Información pública disponible acerca de nuevas vulnerabilidades y exploits.
- Validar con el personal y terceros los reportes de anomalías identificadas y/o reportadas.

B2. Priorización del Manejo del Incidente.

Los incidentes no deben manejarse por orden de llegada como resultado de las limitaciones de recursos. En cambio, el manejo debe priorizarse en función de los factores relevantes.

- Impacto funcional del incidente.
- Información a la que afecta el incidente.
- Recursos necesarios para la recuperación del incidente.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Categorías de Impacto Funcional.

Categoría	Definición
Ninguna	No afecta la capacidad del Instituto FONACOT para proporcionar todos los servicios.
Bajo	Efecto mínimo, el Instituto FONACOT aún puede proporcionar todos los servicios, pero ha perdido eficiencia.
Medio	El Instituto FONACOT ha perdido la capacidad de proporcionar servicios de manera eficiente a uno o más procesos críticos.
Alto	El Instituto FONACOT ya no puede proporcionar servicios a uno o más procesos críticos.

Categorías que Afecta el Incidente a la Información.

Categoría	Definición
Ninguna	Ninguna información fue filtrada, modificada, eliminada o comprometida.
Brecha en la privacidad	Se accedió o se filtró información confidencial de identificación personal de clientes, personal, etc.
Brecha en la propiedad	Se accedió o se filtró información no clasificada, como información de infraestructura crítica protegida.
Pérdida de integridad	La información confidencial o de propiedad se modificó o eliminó.

Categorías de los Recursos Necesarios para la Recuperación del Incidente.

Categoría	Definición
Regular	El tiempo de recuperación es predecible con los recursos existentes.
Complementada	El tiempo de recuperación es predecible con recursos adicionales.
Extendida	El tiempo de recuperación es impredecible; se necesitan recursos adicionales y ayuda externa.
No recuperable	La recuperación del incidente no es posible (datos confidenciales extraídos y publicados públicamente); iniciar investigación.

B3. Informar del Incidente al Personal Laboral y Externos.

El ERISC del Instituto FONACOT, debe notificar a las personas apropiadas para que todos los que necesiten participar desempeñen sus funciones. De manera adicional, de acuerdo con el análisis y priorización del incidente, se debe informar a los siguientes participantes:

- Otros equipos de respuesta a incidentes dentro del Instituto FONACOT como puede ser recursos materiales.
- Equipos externos de respuesta a incidentes.
- Dirección de la Unidad Administrativa que es custodio del sistema.
- Recursos humanos, para casos que involucran al personal laboral.
- Relaciones públicas, para incidentes que pueden generar publicidad negativa del Instituto FONACOT.
- Departamento legal, para incidentes con posibles implicaciones legales.
- Policía cibernética, Seguridad Pública, Ministerio Público.

El Instituto FONACOT debe contar con varios canales de comunicación y seleccionando los que sean apropiados para un incidente en particular. Los posibles canales de comunicación son:

- Correo electrónico.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Sitio web (interno o externo).
- Llamadas telefónicas.
- En persona.
- Buzón de voz.

C. Respuesta y Recuperación.

C1. Contención del Incidente.

El Instituto FONACOT debe definir riesgos aceptables en el manejo de incidentes y desarrollar diferentes estrategias de contención, mismas que ayuden en la toma de decisiones (apagar un sistema, desconectarlo de una red, desactivar ciertas funciones).

Los criterios para determinar la estrategia apropiada incluyen:

- Daño potencial y robo de recursos.
- Necesidad de preservación de evidencia.
- Disponibilidad del servicio (conectividad de red, servicios prestados a terceros).
- Tiempo y recursos necesarios para implementar la estrategia.
- Efectividad de la estrategia (contención parcial, contención total).
- Duración de la solución
 - Solución de emergencia que se eliminará en 4 horas.
 - Solución temporal que se eliminará en dos semanas.
 - Solución permanente.

C2. Adquisición, Preservación, Aseguramiento y Documentación de Evidencia.

El Instituto FONACOT debe documentar claramente cómo se han conservado todas las pruebas, incluidos los sistemas comprometidos. La evidencia debe recopilarse de acuerdo con los procedimientos que cumplan con todas las leyes y regulaciones aplicables que se han desarrollado a partir de discusiones previas con la Dirección de Contraloría Interna, agencias federales y locales de ciberseguridad, esto con la finalidad de que cualquier evidencia pueda ser admisible en caso de iniciar algún juicio penal.

La evidencia debe ser contabilizada en todo momento; siempre que se transfieran pruebas de una persona a otra, los formularios de cadena de custodia deben detallar la transferencia e incluir la firma de cada parte.

Se debe mantener un registro detallado de todas las pruebas, incluidas las siguientes:


- Información de identificación (por ejemplo, la ubicación, número de serie, número de modelo, nombre de host, direcciones de control de acceso a medios (MAC) y direcciones IP de una computadora).
- Nombre, título y número de teléfono de cada persona que recopiló o manejó la evidencia durante la investigación.
- Hora y fecha (incluida la zona horaria) de cada caso de manejo de evidencia.
- Lugares donde se almacenaron las pruebas.

La evidencia debe recolectarse tan pronto como se sospeche que puede haber ocurrido un incidente.

C3. Erradicación y Recuperación del Incidente.

Se deben eliminar los componentes del incidente, como eliminar el malware y deshabilitar las cuentas vulneradas, así como identificar y mitigar todas las vulnerabilidades que se explotaron.

Se deben identificar todos los servidores afectados dentro del Instituto FONACOT para que puedan ser remediados.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

En la recuperación, los administradores deben restaurar los sistemas a su funcionamiento normal, confirmando que los sistemas funcionan normalmente y (si corresponde) corregir vulnerabilidades para evitar incidentes futuros similares.

La recuperación en caso de ser necesario debe considerar la restauración de sistemas a partir de copias de seguridad limpias, reconstruir el ambiente desde cero, reemplazar archivos comprometidos con versiones seguras, instalar parches, cambiar contraseñas y ajustar la seguridad del perímetro de la red (por ejemplo, reglas de firewall, listas de control de acceso de enrutador de límite).

La erradicación y la recuperación deben realizarse bajo un enfoque gradual, teniendo priorizados los pasos de remediación.

C4. Lecciones Aprendidas.

El Instituto FONACOT debe capitalizar el conocimiento adquirido derivado de las incidencias que se presenten y mejorar los aspectos previos, durante y al término de un incidente.

Después de cada incidente importante debe celebrarse una reunión de "lecciones aprendidas" con todas las partes involucradas y opcionalmente de manera periódica para incidentes menores, en dichas sesiones se deben enfocar a mejorar las medidas de seguridad y el proceso de gestión de incidentes.

Los puntos mínimos por considerar en la reunión incluyen:

- ¿Exactamente qué sucedió y a qué hora?
- ¿Qué tan bien se desempeñó el personal laboral y la gerencia en el manejo del incidente?
- ¿Se siguieron los procedimientos documentados? ¿Eran adecuados?
- ¿Qué información se necesitaba al inicio de la incidencia?
- ¿Qué deberían hacer de manera diferente el personal laboral y la gerencia la próxima vez que ocurra un incidente similar?
- ¿Cómo podría mejorarse el intercambio de información con otros equipos (internos, externos)?
- ¿Qué acciones correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué precursores o indicadores deberían observarse en el futuro para detectar incidentes similares?
- ¿Qué herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar futuros incidentes?

El RSI en conjunto con el ERISC deben identificar e indicar las acciones necesarias para la implementación o rediseño de controles automatizados o manuales, así como la actualización de políticas y procedimientos relacionados con la respuesta de incidentes.

Se debe realizar un análisis post-incidente de la forma en que se manejó el incidente con la finalidad de identificar actividades faltantes o inexactitud en algún procedimiento.

Posterior a cada incidente se requiere la creación de un informe de seguimiento, el informe debe servir de referencia para ayudar a manejar incidentes similares. Dicho informe debe incluir la cronología de los eventos (incluida la información con marca de tiempo, como los datos de registro de los sistemas), estimación monetaria de la cantidad de daño que causó el incidente.

Los informes de seguimiento deben mantenerse durante el período de tiempo que se especifica en la Política de Gestión de Activos de la Información.

C5. Uso de Datos de Incidentes Recopilados.

Los datos de incidentes recopilados deberían ser utilizados para:

- Registrar las horas totales de participación y el costo del incidente.
- Analizar las características del incidente identificando debilidades y amenazas de seguridad.
- Conocer cambios en las tendencias por tipo de incidente.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

De manera adicional, los datos deben ser considerados en el análisis de riesgos tecnológicos y realizar una corrida para actualizar el mapa de riesgos.

Las métricas para los datos relacionados con el incidente incluyen:

- Número de incidentes reportados.
- Tiempo por incidente.
 - Cantidad total de trabajo dedicado a trabajar en el incidente.
 - Tiempo transcurrido desde el comienzo del incidente hasta el descubrimiento del incidente, la evaluación de impacto inicial y cada etapa del proceso de manejo del incidente (contención, recuperación).
 - Cuánto tiempo le tomó al equipo de respuesta a incidentes responder al informe inicial del incidente.
 - Cuánto tiempo llevó informar el incidente a la administración y, si es necesario, a las entidades externas correspondientes.
- Evaluación objetiva de cada incidente.
 - Revisión de registros, formularios, informes y otra documentación de incidentes para el cumplimiento de las políticas y procedimientos establecidos de respuesta a incidentes.
 - Identificar qué precursores e indicadores del incidente se registraron para determinar qué tan efectivamente se registró e identificó el incidente.
 - Determinar si el incidente causó daños antes de ser detectado.
 - Determinar si se identificó la causa real del incidente e identificar el vector de ataque, las vulnerabilidades explotadas y las características de los sistemas, redes y aplicaciones objetivo o victimizado.
 - Determinar si el incidente es una recurrencia de un incidente anterior.
 - Calcular el daño monetario estimado del incidente (por ejemplo, información y procesos comerciales críticos afectados negativamente por el incidente).
 - Medir la diferencia entre la evaluación de impacto inicial y la evaluación de impacto final.
 - Identificar qué medidas, de haberlas, podrían haber evitado el incidente.
- Evaluación subjetiva de cada incidente.
 - Políticas, planes y procedimientos de respuesta a incidentes.
 - Herramientas y recursos.
 - Modelo y estructura del equipo.
 - Capacitación y educación sobre el manejo de incidentes.
 - Documentación e informes de incidentes.

D. Actualización y Mejora Continua Institucional.

D1. Implementación de un MGSi.

El Instituto FONACOT desarrollará e implementará un MGSi, conforme 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, publicado en el D.O.F. el 06 de septiembre de 2021.

D2. Implementación de Herramientas de Monitoreo y Detección de Incidentes.

El Instituto FONACOT debe contar con herramientas/tecnologías para el monitoreo y detección de incidentes de seguridad, en caso de no poder contar con dichas herramientas/tecnologías debe justificar la razón de esta.

D3. Capacitación Especializada Continua a los Equipos de Respuesta.

El Instituto FONACOT, en su plan anual de concientización en seguridad de la información, debe contemplar temas de respuesta a incidentes que será divulgado a los equipos de respuesta que cuenta, esto con el fin de mejorar la respuesta al incidente.

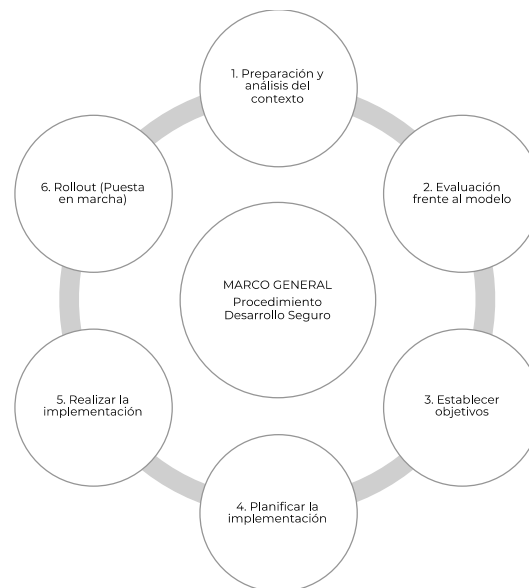
36. PROCEDIMIENTO DE DESARROLLO SEGURO.

1. INTRODUCCIÓN.

El MGSi requiere que exista un ambiente de control de seguridad de la información sobre el desarrollo seguro de aplicaciones.

2. DESARROLLO SEGURO.

2.1. Marco General del Procedimiento de Desarrollo Seguro.



2.1.1. Preparación y Análisis de Contexto.

Propósito.

- Asegurar inicio adecuado del proyecto.

Actividades.

- Definir el alcance – Establecer el objetivo del esfuerzo: todo el Instituto FONACOT, una aplicación o proyecto en particular, un equipo en particular.
- Identificar a los interesados - Asegurar que los interesados importantes estén identificados y alineados para apoyar el proyecto.
- Comunicar - Asegurar que las partes interesadas estén informadas.

2.1.2. Evaluación Frente al Modelo.

Propósito.

- Identificar y comprender cada una de las actividades del plan de seguridad de software.

Actividades.

- Evaluar las actividades actuales - Organice entrevistas con las partes involucradas para comprender el estado actual de las actividades dentro del Instituto FONACOT.
- Determinar el nivel de madurez - En función del resultado, determinar para cada actividad de seguridad el nivel de madurez y determinar la brecha con relación al estado deseado.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.1.3. Establecer Objetivos.

Propósito.

- Desarrollar un puntaje objetivo que se pueda usar para medir las actividades más importantes.

Actividades.

- Definir el objetivo - Establecer o actualizar el objetivo identificando qué actividades del Instituto FONACOT se debería implementar idealmente. Hay que asegurar que el conjunto total de actividades seleccionadas tenga sentido y dependencias entre actividades.
- Estimar el impacto general - Estimar el impacto del objetivo elegido en el Instituto FONACOT. Expresar en argumentos presupuestarios.

2.1.4. Planificar la Implementación.

Propósito.

- Desarrollar o actualizar el plan para llevar al Instituto FONACOT al siguiente nivel respecto a la seguridad en el desarrollo de aplicaciones de software.

Actividades.

- Determinar el cronograma de cambios – Elegir una estrategia de cambio realista en términos de número y duración de fases. Una hoja de ruta típica consta de 4 a 6 fases durante 3 a 12 meses.
- Desarrollar / actualizar el plan de la hoja de ruta - Distribuir la implementación de actividades adicionales en las diferentes fases de la hoja de ruta, teniendo en cuenta el esfuerzo requerido para implementarlas. Equilibrar el esfuerzo de implementación en los diferentes periodos, teniendo en cuenta las dependencias entre actividades.

2.1.5. Realizar la Implementación.

Propósito.

- Administrar la planificación.

Actividades.

- Implementar actividades – Implementación de todas las actividades que forman parte del período. Considerar el impacto en los procesos, las personas, el conocimiento y las herramientas.

2.1.6. Rollout (Puesta en marcha).

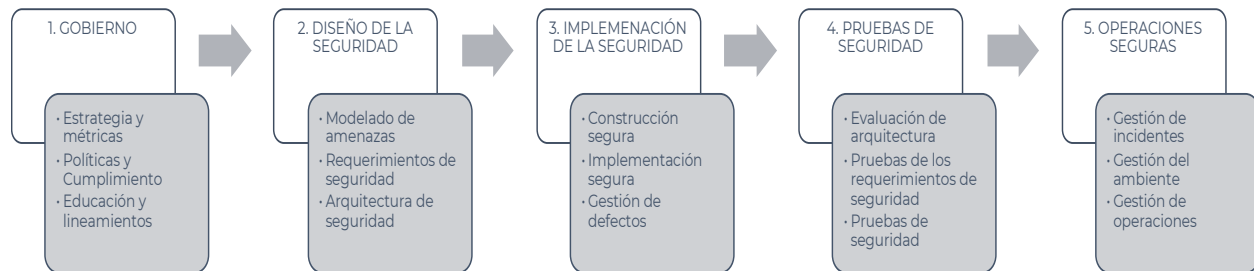
Propósito.

- Validar que las mejoras en la seguridad para el proceso de desarrollo estén disponibles y se utilicen efectivamente dentro del Instituto FONACOT.

Actividades.

- Evangelizar mejoras – Hacer que los pasos y las mejoras sean visibles para todos los involucrados mediante capacitación y sensibilización.
- Medir la efectividad - Medir la adopción y la efectividad de las mejoras implementadas mediante el análisis del uso y el impacto.

2.2. PROCEDIMIENTO DE DESARROLLO SEGURO.



2.2.1. Gobierno (Requerimientos de Seguridad).

- Estrategia y métricas.
 - Definir métricas con información sobre la efectividad y la eficiencia del programa de seguridad de aplicaciones.
 - Establecer objetivos y KPI para medir la efectividad del programa.
 - Estrategia basada en las métricas y las necesidades de la organización.
- Políticas y cumplimiento.
 - Identificar controles y requisitos de cumplimiento indicados en políticas y estándares existentes.
 - Requisitos específicos de cumplimiento y guía de pruebas.
 - Medición y reporte del cumplimiento de los requisitos.
- Educación y lineamientos.
 - Ofrecer al personal laboral acceso a recursos en torno a los temas de desarrollo e implementación seguros.
 - Educar a todo el personal laboral en el ciclo de vida del software con tecnología y orientación específica de roles sobre desarrollo seguro.
 - Desarrollar programas de capacitación internos creados por los desarrolladores de los diferentes equipos involucrados en la solución.

2.2.2. Diseño de la Seguridad.

- Modelado de amenazas.
 - Realizar evaluación de riesgos de la aplicación para comprender la probabilidad y el impacto de un ataque.
 - Comprender el riesgo para todas las aplicaciones en la organización al centralizar el inventario de perfil de riesgo para las partes interesadas.
 - Revisión periódica de los perfiles de riesgo de la aplicación a intervalos regulares para garantizar la precisión y reflejar el estado actual.
- Requerimientos de seguridad.
 - Los objetivos de seguridad de aplicaciones de alto nivel se deben asignar a requerimientos funcionales.
 - Los requisitos de seguridad deben estar disponibles y ser utilizados por los equipos de desarrollo.
 - Desarrollar un marco de requisitos para que los equipos de desarrollo lo utilicen.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Arquitectura de seguridad.
 - Consideraciones de seguridad en el proceso de diseño de software.
 - Proceso de diseño de software enfocado hacia servicios seguros.
 - Proceso de diseño de software y validación de la utilización de componentes seguros.

2.2.3. Implementación de Seguridad.

- Construcción segura.
 - Definición formal del proceso de compilación para que sea coherente y repetible.
 - Identificar dependencias y prever reacciones oportunas a situaciones que supongan un riesgo a las aplicaciones.
 - Comprobaciones de seguridad al proceso de compilación y prever que la creación de artefactos no falle.
- Implementación segura.
 - Formalizar el proceso de implementación y asegurar las herramientas y procesos utilizados.
 - Automatizar el proceso de implementación en todas las etapas e introducir pruebas de verificación de seguridad.
 - Verificar (con herramientas) la integridad de todo el software implementado.
- Gestión de defectos.
 - Seguimiento estructurado de defectos de seguridad y toma de decisiones informadas basadas en esta información.
 - Evaluar todos los defectos de seguridad en toda la organización y definir los SLA.
 - Aplicar los SLA definidos.

2.2.4. Pruebas de Seguridad.

- Evaluación de arquitectura.
 - Identificar los componentes de la arquitectura de aplicaciones e infraestructura y revisión del aprovisionamiento básico de seguridad.
 - Validación de mecanismos de seguridad de la arquitectura.
 - Revisión de la efectividad de los componentes de la arquitectura.
- Pruebas de los requerimientos de seguridad.
 - Análisis de vulnerabilidades periódicas y otros problemas de seguridad.
 - Revisión de implementación para identificar los riesgos específicos de la aplicación respecto a los requisitos de seguridad.
 - Mantener el nivel de seguridad de la aplicación después de la corrección de errores, cambios o durante el mantenimiento.
- Pruebas de seguridad (AST o DAST).
 - Realizar pruebas de seguridad para descubrir defectos de seguridad.
 - Ejecución de SAST y DAST.
 - Configuración de reglas, filtrado de falsos positivos.
 - Automatización de procesos, tableros de control y los KPI.
 - Realizar pruebas de penetración durante el desarrollo.
 - Ejecución de pruebas de penetración Black-box, White-box y Gray-box.
 - Realizar pruebas de seguridad como parte de los procesos de desarrollo e implementación.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- Correlación de pruebas automatizadas y manuales.

2.2.5. Operaciones Seguras.

- Gestión de incidentes.
 - Utilizar los datos de registro disponibles para realizar la mejor detección de posibles incidentes de seguridad.
 - Seguir el proceso establecido y documentado para la detección de incidentes, con énfasis en la evaluación automatizada de registros.
 - Utilizar el proceso de gestión de incidentes.
- Gestión del ambiente.
 - Mejorar el hardening de las configuraciones.
 - Realizar hardening de configuraciones.
 - Monitoreo de las configuraciones y llevar a cabo la gestión de ocurrencias detectadas como defectos de seguridad.
- Gestión de operaciones.
 - Implementación de mejores prácticas en la protección de datos.
 - Desarrollo de catálogo de datos y establecer una política de protección de datos.
 - Automatizar la detección de incumplimiento de políticas y auditar el cumplimiento periódico del catálogo de datos y de la política de protección de datos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

37. PROCEDIMIENTO DE INSTALACIÓN DE PARCHES EN BASES DE DATOS.

1. INTRODUCCIÓN.

El Instituto FONACOT está consciente que en los últimos años los incidentes de seguridad relacionados con la confidencialidad de la información se han producido con mayor frecuencia, aunado a la naturaleza de los servicios que presta. Esto hace que gran parte de la información crítica sea sustentada por bases de datos, lo que resalta la necesidad de contar con seguridad de la información en bases de datos.

El propósito de este procedimiento es establecer un procedimiento estándar para la instalación de la última versión del manejador de bases de datos.

2. INSTALACIÓN DE PARCHES EN BASES DE DATOS.

- **Identificación de activos y software:** Se debe llevar a cabo la identificación de servidores y bases de datos instaladas, así como el nivel de parches de seguridad aplicados, de manera que los cambios se realicen sin riesgos y en caso de producirse algún problema en la actualización o aplicación de parches de seguridad, se permita volver a un estado previo conocido y funcional.
- **Disponibilidad:** Se debe tener un inventario actualizado de servidores y bases de datos, adicionalmente se debe revisar el listado de actualizaciones y parches de seguridad disponibles e identificar cuál de ellos afecta a cada servidor y base de datos.
- **Aplicabilidad:** Las actualizaciones y parches de seguridad publicados no siempre son válidos para todos los equipos, por lo que se debe verificar si la actualización o parche de seguridad son viables.
- **Adquisición:** Se deben obtener los archivos de actualización, así como los parches de seguridad de una fuente confiable.
- **Validación:** Asegurar que la actualización y/o aplicación de parches no impacta de manera negativa la confidencialidad, integridad o disponibilidad de los sistemas de información. Para tal efecto se deben realizar comprobaciones sobre las implicaciones de la actualización o aplicación de parches de seguridad.
- **Despliegue:** Durante el proceso de validación se debe crear un paquete de despliegue. El paquete debe contener el/los archivos de actualización o parches y las instrucciones de instalación, así como un listado de los servidores y bases de datos en los que realizará el despliegue.

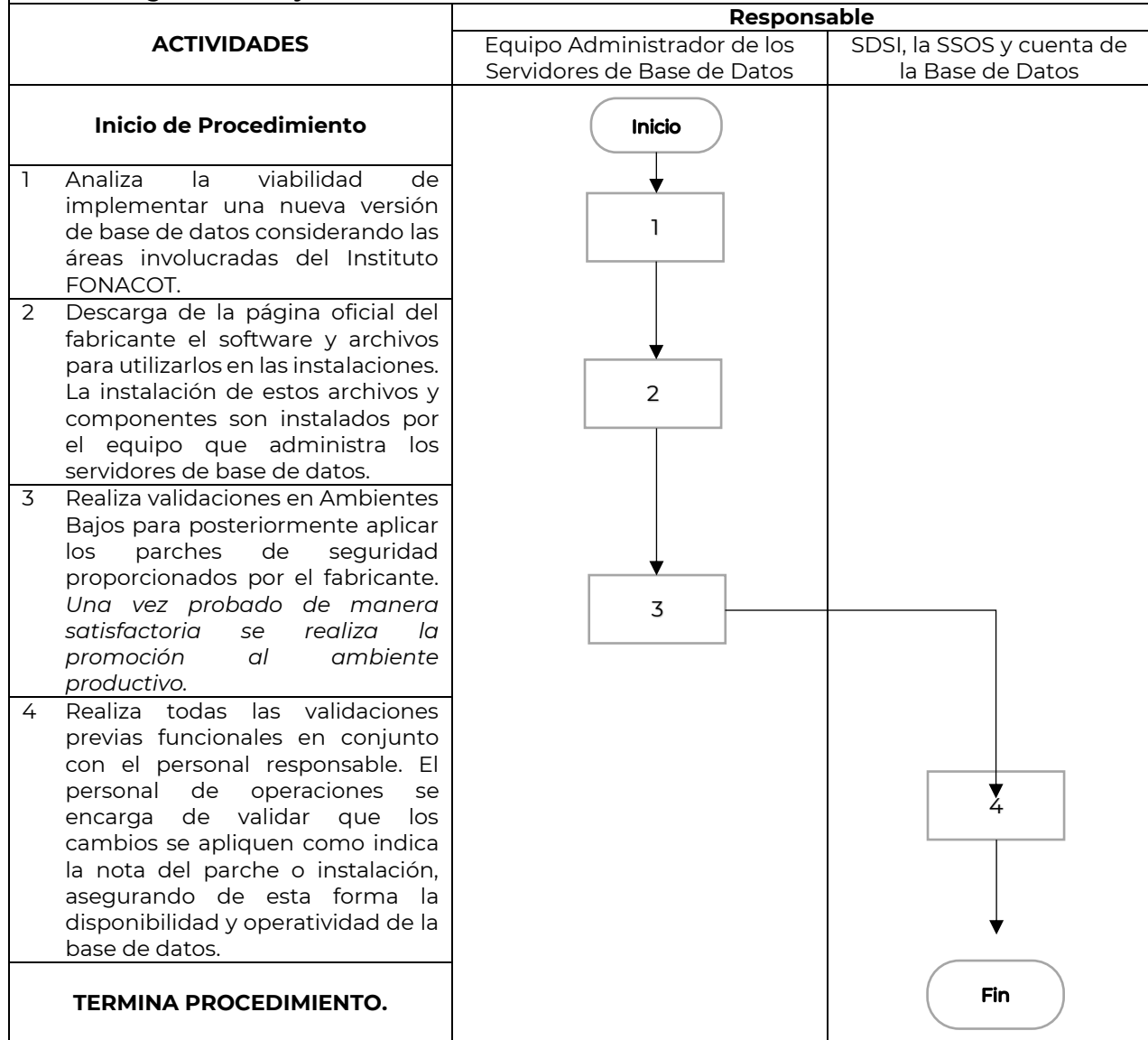
3. DESARROLLO.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
Equipo Administrador de los Servidores de Base de Datos	1. Analiza la viabilidad de implementar una nueva versión de base de datos considerando las áreas involucradas del Instituto FONACOT, esto debido a que para hacer una actualización se deben realizar pruebas por el área de desarrollo y el personal que realiza operaciones en las funcionalidades instaladas o implementadas, esto para verificar que con una actualización de la base de datos no se vean afectadas todas estas funcionalidades.	Manejador de Base de Datos
Equipo Administrador de los Servidores de Base de Datos	2. Descarga de la página oficial del fabricante el software y archivos para utilizarlos en las instalaciones, el acceso es mediante la suscripción que otorga la licencia de la base de datos, es decir, desde este sitio oficial se pueden obtener los archivos de instalación, parches de seguridad, parches para corrección de bugs y adicionalmente tener acceso al área de soporte por el fabricante. La instalación de estos archivos y componentes son instalados por el equipo que administra los servidores de base de datos.	Manejador de Base de Datos Archivos e Instalación
Equipo Administrador de	3. Realiza validaciones en Ambientes Bajos para posteriormente aplicar los parches de seguridad	Matriz de Pruebas

Responsable	Descripción de la actividad	Documento o Producto Involucrado
los Servidores de Base de Datos	proporcionados por el fabricante, ya que se debe considerar la posible afectación a código para la funcionalidad de aplicativos y/o servicios que consumen la base de datos, con la finalidad de asegurar que las funcionalidades liberadas no tengan ninguna afectación. Una vez probado de manera satisfactoria se realiza la promoción al ambiente productivo.	
SDSI, la SSOS y la cuenta de la Base de Datos	4. Realiza todas las validaciones previas funcionales en conjunto con el personal responsable. Con lo anterior, verifica la no afectación de la implementación de una nueva versión de base de datos. El personal de operaciones se encarga de validar que los cambios se apliquen como indica la nota del parche o instalación, asegurando de esta forma la disponibilidad y operatividad de la base de datos.	Matriz de Pruebas
TERMINA PROCEDIMIENTO.		



Diagrama de Flujo del Procedimiento de Instalación de Parches en Bases de Datos.



38. PROCEDIMIENTO DE CONTROL DE SEGUIMIENTO A VULNERABILIDADES.

1. INTRODUCCIÓN.

El Instituto FONACOT realizará la identificación, seguimiento, control y atención de vulnerabilidades técnicas sobre los sistemas de información y equipos informáticos, a través de un procedimiento de control de seguimiento a vulnerabilidades con el propósito de mantener un nivel adecuado de la seguridad de la información en las plataformas tecnológicas y mitigar las vulnerabilidades asociadas.

2. CONTROL DE SEGUIMIENTO A VULNERABILIDADES.

- Únicamente el RSI puede realizar la solicitud de los análisis de vulnerabilidades que sean necesarios, sobre la infraestructura del Instituto FONACOT, aplicaciones web, aplicaciones móviles y cualquier otro activo que considere necesario.
- Todos los análisis de vulnerabilidades deben tener un ID único con el cual se administre la trazabilidad de la vulnerabilidad respecto al activo asociado.
- Se debe integrar un reporte del resultado del análisis de vulnerabilidades indicando el detalle, la criticidad, urgencia y las recomendaciones de remediación.
- Se debe contar con bitácoras de todos los análisis de vulnerabilidades realizados.

3. DESARROLLO.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
RSI	1. Elabora el programa anual de análisis de vulnerabilidades.	Programa Anual de Análisis de Vulnerabilidades
RSI	2. Realiza de manera formal la realización de los análisis de vulnerabilidades respecto con el calendario establecido.	Programa Anual de Análisis de Vulnerabilidades
RSI	3. Realiza el análisis de vulnerabilidades y su documentación.	Análisis de Vulnerabilidades
RSI	4. Envía a las áreas correspondientes el detalle, la criticidad y urgencia de corrección, incluyendo recomendaciones de corrección a las vulnerabilidades detectadas.	Plan de Remediación
Personal del Área Involucrada del Instituto FONACOT	5. Analiza la sugerencia de corrección para su implementación y presenta la estrategia y planeación para la atención a las vulnerabilidades. a. El plan de Remediación incluye lo siguiente: b. Fecha de inicio y terminación de la remediación. c. Persona líder y equipo responsable. d. Ruta crítica. e. Criterios de pruebas y aceptación. f. Presupuesto que llegara a ser necesario. <i>En caso de que la vulnerabilidad no pueda remediarse, se da justificación correspondiente.</i>	Plan de Remediación Justificación
Personal del Área Involucrada del Instituto FONACOT	6. Implementa la solución o justificación respecto con la vulnerabilidad notificada.	Plan de Remediación Justificación
RSI	7. Revisa que en la remediación de vulnerabilidades se hayan realizado las pruebas necesarias, considerando todos los escenarios bajo los cuales fue detectada la vulnerabilidad y que los resultados	Pruebas de Remediación

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Responsable	Descripción de la actividad	Documento o Producto Involucrado
	obtenidos hayan sido satisfactorios. Así mismo, confirma la solución de las vulnerabilidades o en su caso aprueba la justificación que aplique.	
RSI	8. Realiza el control sobre el seguimiento de las vulnerabilidades con la finalidad de analizar la recurrencia por tipo de vulnerabilidad y el tiempo de atención con relación a la criticidad de la vulnerabilidad.	Seguimiento a Vulnerabilidades
TERMINA PROCEDIMIENTO.		



Diagrama de Flujo del Procedimiento de Control de Seguimiento a Vulnerabilidades.

ACTIVIDADES	Responsable	
	RSI	Personal del Área Involucrada del Instituto FONACOT
Inicio de Procedimiento	<pre> graph TD Inicio([Inicio]) --> 1[1] 1 --> 2[2] 2 --> 3[3] 3 --> 4[4] 4 --> 5[5] 5 --> 6[6] 6 --> 7[7] 7 --> 8[8] 8 --> Fin([Fin]) </pre>	
1 Elabora el programa anual de análisis de vulnerabilidades.		
2 Realiza de manera formal la realización de los análisis de vulnerabilidades respecto con el calendario establecido.		
3 Realiza el análisis de vulnerabilidades y su documentación.		
4 Envía a las áreas correspondientes el detalle, la criticidad y urgencia de corrección, incluyendo recomendaciones de corrección a las vulnerabilidades detectadas.		
5 Analiza la sugerencia de corrección para su implementación y presenta la estrategia y planeación para la atención a las vulnerabilidades. En caso de que la vulnerabilidad no pueda remediarse, se da justificación correspondiente.		
6 Implementa la solución o justificación respecto con la vulnerabilidad notificada.		
7 Revisa que en la remediación de vulnerabilidades se hayan realizado las pruebas necesarias, considerando todos los escenarios bajo los cuales fue detectada la vulnerabilidad y que los resultados obtenidos hayan sido satisfactorios. Así mismo, confirma la solución de las vulnerabilidades o en su caso aprueba la justificación que aplique.		
8 Realiza el control sobre el seguimiento de las vulnerabilidades con la finalidad de analizar la recurrencia por tipo de vulnerabilidad y el tiempo de atención con relación a la criticidad de la vulnerabilidad.		
TERMINA PROCEDIMIENTO.		

39. PROCEDIMIENTO DE POLÍTICAS DE COMUNICACIÓN.

1. INTRODUCCIÓN.

El Instituto FONACOT garantiza el acceso autorizado a los recursos y servicios tecnológicos a través de la gestión y límites en las políticas de comunicación, así también niega el acceso cuentas no autorizadas.

2. POLÍTICAS DE COMUNICACIÓN.

- Únicamente la DIT puede realizar la solicitud de reglas de firewall para el personal interno y externos que tengan alguna relación justificada para hacer uso de los recursos y servicios tecnológicos del Instituto FONACOT.
- Todas las solicitudes de reglas de firewall deben gestionarse a través del “Formato de solicitud de reglas de comunicación”.
- La DIT es responsable de llenar el formato en su totalidad y posteriormente enviarlo al RSI.
- El RSI recibe y evalúa el requerimiento. Posteriormente acepta o declina la solicitud conforme a la justificación, descripción técnica, criterios de seguridad y riesgo asociado.

3. DESARROLLO.

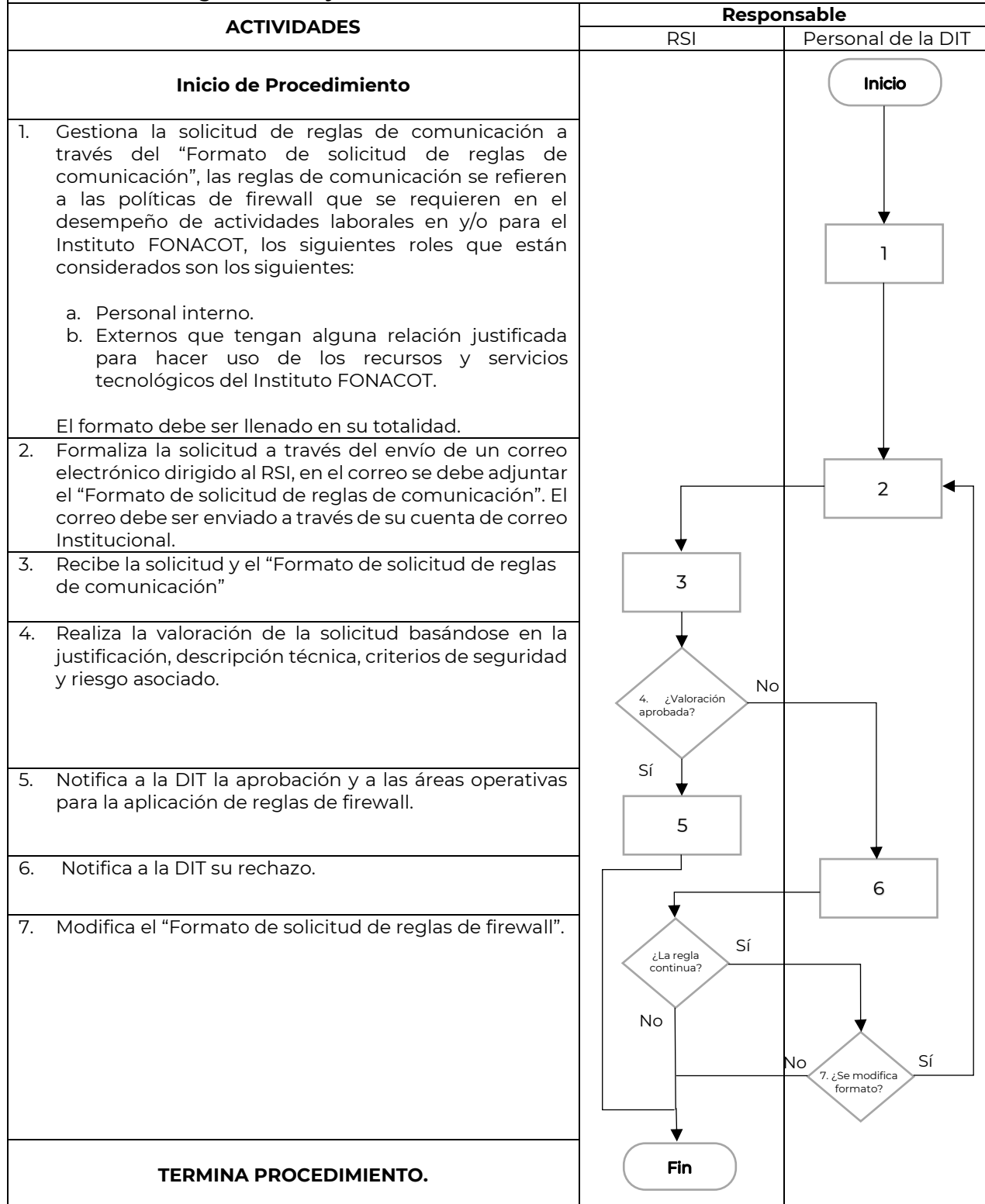
Responsable	Descripción de la actividad	Documento o Producto Involucrado
Personal de la DIT	1. Gestiona la solicitud de reglas de comunicación a través del “Formato de solicitud de reglas de comunicación”, las reglas de comunicación se refieren a las políticas de firewall que se requieren en el desempeño de actividades laborales en y/o para el Instituto FONACOT, los siguientes roles que están considerados son los siguientes: <ol style="list-style-type: none"> Personal interno. Externos que tengan alguna relación justificada para hacer uso de los recursos y servicios tecnológicos del Instituto FONACOT. El formato debe ser llenado en su totalidad.	Formato de Solicitud de Reglas de Comunicación
Personal de la DIT	2. Formaliza la solicitud a través del envío de un correo electrónico dirigido al RSI, en el correo se debe adjuntar el “Formato de solicitud de reglas de comunicación”. El correo debe ser enviado a través de su cuenta de correo Institucional	Solicitud de Reglas de Firewall Formato de Solicitud de Reglas de Comunicación
RSI	3. Recibe la solicitud y el “Formato de solicitud de reglas de comunicación”	Solicitud de Reglas de Firewall Formato de Solicitud de Reglas de Comunicación
RSI	4. Realiza la valoración de la solicitud basándose en la justificación, descripción técnica, criterios de seguridad y riesgo asociado	Solicitud de Reglas de Firewall Formato de Solicitud de Reglas de Comunicación
RSI	<i>Si de la valoración resulta que la solicitud es Aprobada, Continúa Actividad 5.</i> 5. Notifica a la DIT la aprobación y a las áreas operativas para la aplicación de reglas de firewall. Termina Procedimiento.	Solicitud de Reglas de Firewall Formato de Solicitud de Reglas de Comunicación

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Responsable	Descripción de la actividad	Documento o Producto Involucrado
RSI	<i>Si de la valoración resulta que la solicitud No es Aprobada, continúa con actividad 6.</i> 6. Notifica a la DIT su rechazo.	Solicitud de Reglas de Firewall Formato de Solicitud de Reglas de Comunicación
Personal de la DIT	<i>Si se determina que la regla de firewall siga siendo requerida, continúa con actividad 7.</i> 7. Modifica el "Formato de solicitud de reglas de firewall". Continúa con Actividad 2, de lo contrario Termina Procedimiento.	Formato de Solicitud de Reglas de Comunicación
TERMINA PROCEDIMIENTO.		



Diagrama de Flujo del Procedimiento de Políticas de Comunicación.



40. PROCEDIMIENTO PARA LA RECEPCIÓN Y ATENCIÓN DE TICKETS DE SEGURIDAD DE LA INFORMACIÓN.

1. INTRODUCCIÓN.

Este procedimiento establece los lineamientos para brindar una atención de manera oportuna y eficiente a los tickets relacionados con problemas e incidentes de ciberseguridad.

2. RECEPCIÓN Y ATENCIÓN DE TICKETS DE SEGURIDAD DE LA INFORMACIÓN.

- Toda solicitud debe presentarse a través de ticket levantado en el 111 - Mesa de Servicio.
- Todos los tickets reasignados a Seguridad de la Información deben contener anexos la evidencia de las acciones llevadas a cabo y por el Área Técnica que solicita la reasignación a través de la mesa de servicio.

3. DESARROLLO.

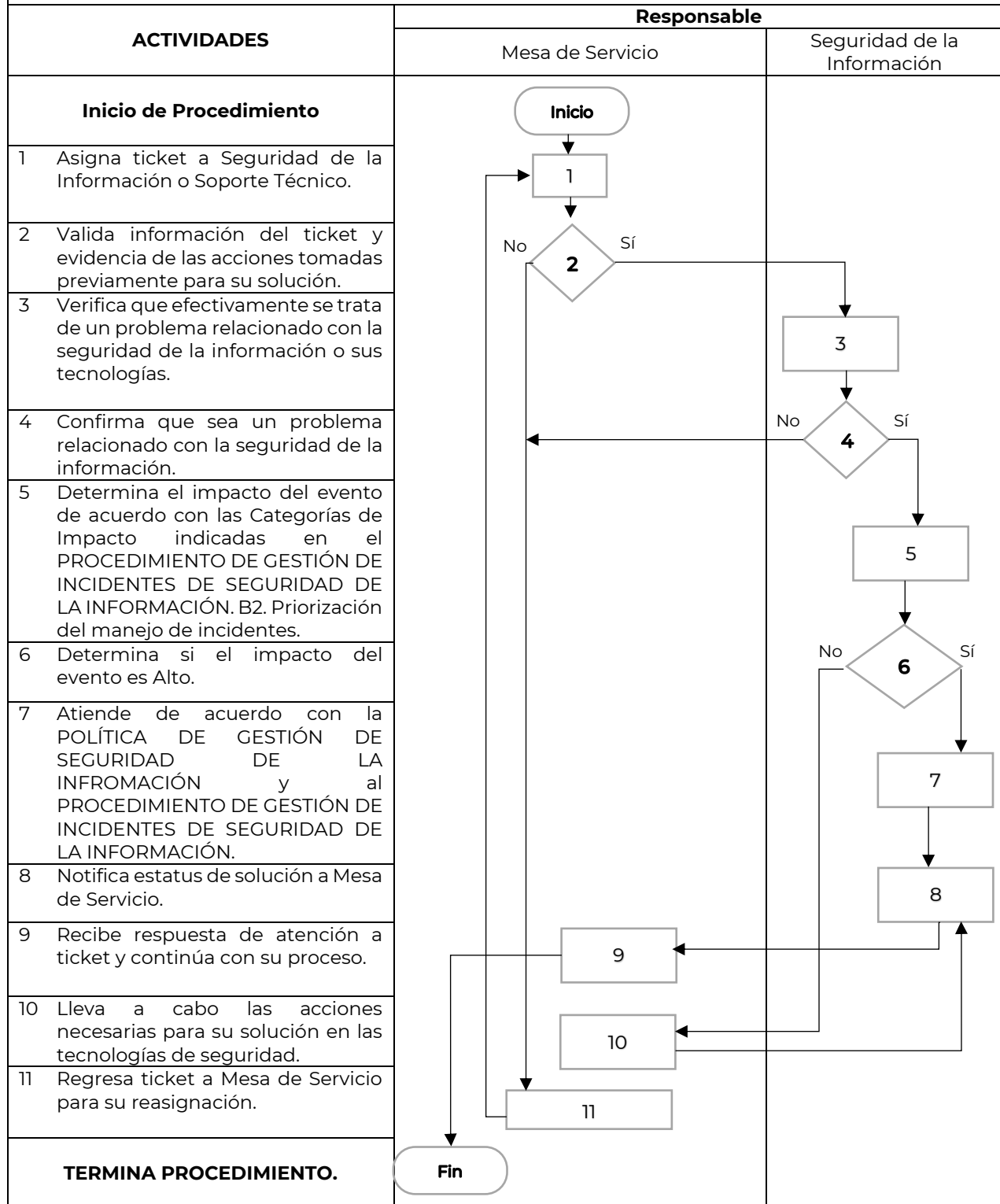
Responsable	Descripción de la Actividad	Documento o Producto Involucrado
Personal de Mesa de Servicio	1. Asigna Ticket a Seguridad de la Información o Soporte Técnico.	Ticket
RSI	2. Valida que el Ticket cuente con evidencia de acciones tomadas para su solución. <i>Si el Ticket cuenta con la información y evidencia necesaria, continua con actividad 3. De lo contrario, continúa con actividad 11.</i>	Ticket Evidencia
RSI	3. Verifica que efectivamente se trata de un problema relacionado con la seguridad de la información o sus tecnologías. Continúa con actividad 4.	Ticket Evidencia
RSI	4. Confirma que sea un problema relacionado con la seguridad de la información. <i>Si se trata de un problema de seguridad de la información, continua con actividad 5. De lo contrario, continúa con actividad 11.</i>	Ticket. Evidencia
RSI	5. Determina el impacto del evento de acuerdo con las Categorías de Impacto indicadas en el PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. B2. Priorización del manejo de incidentes. Continúa con actividad 6.	Ticket Evidencia PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. B2. Priorización del manejo de incidentes.
RSI	6. Determina si el impacto del evento es Alto. <i>Si se determina que el impacto es Alto, continua con actividad 7. De lo contrario, continúa con actividad 10.</i>	Ticket. Evidencia
RSI	7. Atiende de acuerdo con la POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y al PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. Continúa con actividad 8.	Ticket. Evidencia POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y al PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Responsable	Descripción de la Actividad	Documento o Producto Involucrado
RSI	8. Notifica estatus de solución al personal de Mesa de Servicio. Continúa con actividad 9.	Ticket. Evidencia
Personal de Mesa de Servicio	9. Recibe respuesta de atención a ticket y continúa con su proceso interno.	Ticket. Evidencia
RSI Equipo Técnico de las Tecnologías de Ciberseguridad.	10. Lleva a cabo las acciones necesarias para su solución en las tecnologías de seguridad. Continúa con actividad 8.	Ticket. Evidencia
Personal de Mesa de Servicio	11. Regresa ticket a Mesa de Servicio para su reasignación. Continúa con actividad 1.	Ticket. Evidencia
TERMINA PROCEDIMIENTO.		



Diagrama de Flujo del Procedimiento de Recepción y Atención de tickets de Seguridad de la Información.



41. PROTOCOLO DE ATENCIÓN AL FRAUDE DE CLIENTES DEL INSTITUTO FONACOT.

1. INTRODUCCIÓN.

Derivado del creciente número de fraudes a clientes del Instituto FONACOT, se desarrolla un protocolo de atención al fraude para que los clientes, el Instituto FONACOT y otras dependencias del Gobierno Federal atiendan la incidencia en tiempo y forma, así como brindar atención y solución al cliente.

2. ATENCIÓN AL FRAUDE DE CLIENTES DEL INSTITUTO FONACOT.

- El cliente se presenta a la DEPyR a presentar el caso del posible fraude.
- El cliente debe levantar la denuncia correspondiente ante el ministerio público, una vez que haya acudido a la DEPyR.

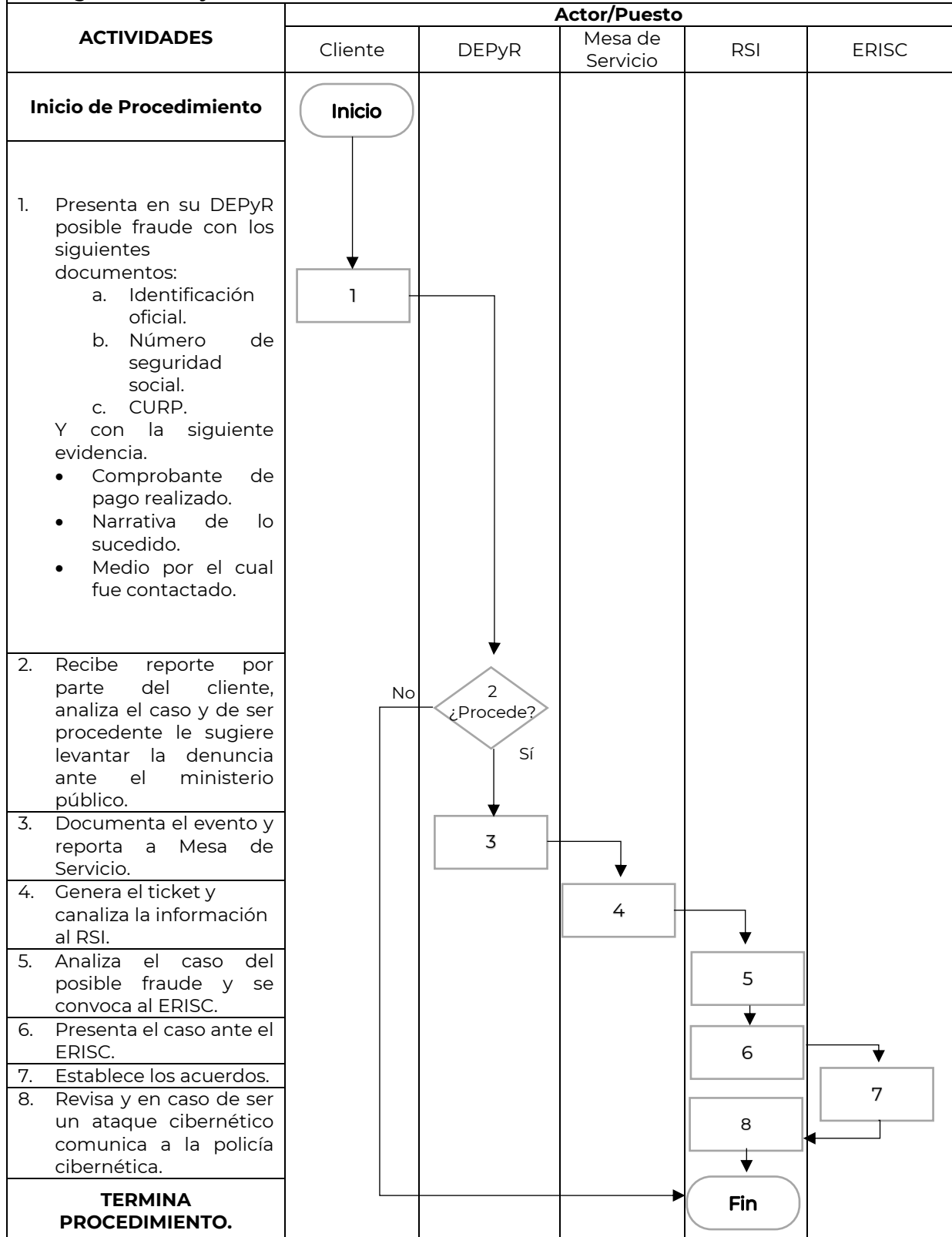
3. DESARROLLO.

3.1 Reporte y Atención.

Responsable	Descripción de la actividad	Documento o Producto Involucrado
Cliente	1. Acude a la DEPyR con la finalidad de reportar el posible fraude.	Identificación Oficial Número de Seguridad Social CURP Comprobante de Pago Realizado Narrativa de lo Sucedido Medio por el cual fue Contactado
DEPyR	2. Recibe reporte por parte del cliente, analiza el caso y de ser procedente le sugiere levantar la denuncia ante el ministerio público.	Reporte de Posible Fraude
DEPyR	3. Documenta el evento y reporta a Mesa de Servicio.	Reporte de Posible Fraude
Personal de Mesa de Servicio	4. Genera el Ticket y canaliza la información al Responsable de Seguridad de la Información	Ticket
RSI	5. Analiza el caso del posible fraude y convoca al ERISC.	Minuta.
RSI	6. Presenta el caso ante el ERISC.	Minuta
ERISC	7. Establece los acuerdos.	Minuta
RSI	8. Revisa y en caso de ser un ataque cibernético comunica a la policía cibernética.	Reporte de Posible Fraude
TERMINA PROCEDIMIENTO.		



Diagrama de Flujo del Protocolo de Atención al Fraude de Clientes del Instituto FONACOT.



 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

42. METODOLOGÍA DE LA EVALUACIÓN DE RIESGOS TECNOLÓGICOS.

1. INTRODUCCIÓN.

La evaluación de riesgos tecnológicos ayuda a la identificación, clasificación y priorización sobre el impacto en activos del Instituto FONACOT (servicios, aplicativos, datos, infraestructura), de tal manera surge la necesidad de definir la metodología para el análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información del Instituto FONACOT.

2. ADMINISTRACIÓN DE RIESGOS.

El proceso de administración de riesgos tecnológicos es coordinado por el RSI, las actividades a realizar son las siguientes:

1. Identificación de los activos y del personal que son sus custodios (inventario de activos).
2. Valoración de los activos con base en las dimensiones de seguridad (C+I+D).
3. Identificación de las amenazas relevantes para cada activo.
4. Valoración de amenazas de acuerdo con:
 - a. Estimación de la probabilidad de ocurrencia de la amenaza sobre cada activo.
 - b. Estimación de la degradación que causaría la amenaza en cada dimensión (C+I+D) del activo si esta llegase a materializarse.
5. Calcular el impacto de la amenaza sobre el activo de información y esto se realiza con base al valor del activo por la degradación (impacto = valor del activo * degradación).
6. Calcular el nivel de riesgo, es el impacto por la probabilidad (riesgo = Impacto * probabilidad).
7. Identificación de la Dirección de la Unidad Administrativa responsable de los riesgos.
8. Gestionar los riesgos:
 - a. Identificar y elegir los controles.
 - b. Valorar la estimación de eficacia de los controles.
9. Realizar el informe de la evaluación de riesgos.
10. Realizar la evaluación del riesgo residual.

3. IDENTIFICACIÓN DE ACTIVOS Y SUS CUSTODIOS.

El primer paso en la evaluación de riesgos es la identificación de todos los activos que procesen, transmitan o guarden información.

Los activos se han agrupado bajo 9 categorías:

- Datos / Información.
- Claves criptográficas.
- Aplicaciones (software).
- Equipamiento informático (hardware).
- Soportes de información.
- Equipamiento auxiliar.
- Instalaciones físicas.
- Personal laboral.
- Contractual.

Los activos deben estar bajo responsabilidad de personal laboral o unidad organizativa del Instituto FONACOT.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.1 Valoración de los Activos.

Para determinar el valor de un activo se consideran tres dimensiones de seguridad que son; (i) confidencialidad, (ii) integridad y (iii) disponibilidad, a cada dimensión se le asigna un valor dependiendo de la criticidad que esta tenga hacia el Instituto FONACOT, la escala a considerar es; muy alto, alto, medio, bajo y muy bajo.

Para obtener el valor del activo es necesario identificar en que dimensión es más valioso, para la adquisición de este conocimiento es necesario llevar a cabo entrevistas con áreas de negocio, operativas y tecnológicas.

A continuación, se presentan los criterios para evaluar las dimensiones de seguridad.

3.1.1 Confidencialidad.

La confidencialidad se evalúa respondiendo la siguiente pregunta:

- **¿Qué daño causaría que lo conociera quien no debe?**

El resultado puede ser el siguiente:

#	Escala	Descripción
1	Muy Bajo	Es probable que no se tenga ningún efecto adverso al Instituto FONACOT.
2	Bajo	Es probable que solo se tenga un efecto mínimo limitado al Instituto FONACOT.
3	Medio	Es probable que se tenga un efecto adverso limitado en el Instituto FONACOT.
4	Alto	Es probable que se tenga un efecto adverso grave en el Instituto FONACOT.
5	Muy Alto	Es probable que se tenga un efecto adverso catastrófico en el Instituto FONACOT.

3.1.2 Integridad.

La integridad se evalúa respondiendo la siguiente pregunta:

- **¿Qué perjuicio causaría que estuviera dañado o corrupto?**

Lo que evalúa es que la información puede estar modificada, ser total o parcialmente falsos o incluso, faltar datos.

El resultado puede ser el siguiente:

#	Escala	Descripción
1	Muy Bajo	Es probable que no se tenga ningún efecto adverso al Instituto FONACOT.
2	Bajo	Es probable que solo se tenga un efecto mínimo limitado al Instituto FONACOT.
3	Medio	Es probable que se tenga un efecto adverso limitado en el Instituto FONACOT.
4	Alto	Es probable que se tenga un efecto adverso grave en el Instituto FONACOT.
5	Muy Alto	Es probable que se tenga un efecto adverso catastrófico en el Instituto FONACOT.

3.1.3 Disponibilidad.

La disponibilidad se evalúa respondiendo la siguiente pregunta:

- **¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?**

El resultado es el siguiente:

#	Escala	Descripción
1	Muy Bajo	Es probable que no se tenga ningún efecto adverso al Instituto FONACOT.
2	Bajo	Es probable que solo se tenga un efecto mínimo limitado al Instituto FONACOT.
3	Medio	Es probable que se tenga un efecto adverso limitado en el Instituto FONACOT.
4	Alto	Es probable que se tenga un efecto adverso grave en el Instituto FONACOT.
5	Muy Alto	Es probable que se tenga un efecto adverso catastrófico en el Instituto FONACOT.

3.2 Calculando el Valor del Activo.

Para tener un valor cuantitativo del activo se realiza la suma de las dimensiones de seguridad (C+I+D) como la siguiente fórmula:

Valor del Activo = Confidencialidad + Integridad + Disponibilidad.

Los resultados de la valoración de los activos es el resultado de la suma de sus dimensiones (C+I+D) es el valor que se le da al activo, como lo representa la siguiente tabla.

Valor del activo [C + I + D]		
5	Muy Alto	Sí, la suma es del 13 al 15.
4	Alto	Sí, la suma es del 10 al 12.
3	Medio	Sí, la suma es del 7 al 9.
2	Bajo	Sí, la suma es del 4 al 6.
1	Muy Bajo	Sí, la suma es igual a 3.

Se utiliza la fórmula en Excel **"=SI (SUMA (D3:F3) <4,1, SI (SUMA (D3:F3) <7,2, SI (SUMA (D3:F3) <10,3, SI (SUMA (D3:F3) <13,4,5)))))"**

Nota: Esta fórmula solo es de referencia, ya que puede variar según las celdas y filas del libro donde se realice el análisis.

Ejemplo de Valoración de un Activo:

Si le asignamos valores a las dimensiones.

Confidencialidad = 1, Disponibilidad = 3 e Integridad = 3

El resultado del valor del activo con base en estas dimensiones sería 1+3+3 = 7, por lo tanto, el valor del activo es Medio (7):

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

C	I	D	Valor del activo
1	3	3	7

Nota: solo se pueden seleccionar valores de 1, 2, 3, 4 y 5 todo valor fuera de estos rangos no está disponible.

Descripción del activo	
Muy Alto	Activos que afectan procesos críticos que no pueden restablecerse en menos de dos días.
Alto	Activos que afectan procesos críticos que pueden restablecerse en menos de dos días.
Medio	Activos que afectan varios procesos no críticos del Instituto FONACOT.
Bajo	Activos que no afectan a los procesos del Instituto FONACOT.

3.2.1 Identificación de la Amenaza.

En esta actividad se identifica todas las amenazas relacionadas con un activo y para ello se considera que activo puede ser propenso o vulnerable a dicha amenaza.

Un activo puede estar relacionado con varias amenazas y una amenaza relacionada con varios activos.

Valoración de la Amenaza.

Para otorgar un valor a la amenaza se considera la probabilidad de ocurrencia que esta tendría sobre el activo y en qué nivel de degradación se vería afectado el activo si la amenaza se materializa.

Factores que influyen en la valoración de que tan probable es que la amenaza se materialice son:

- Incidentes de seguridad que el Instituto FONACOT ha tenido.
- Incidentes de seguridad que han ocurrido en las organizaciones del mismo giro.
- Defectos o fallas reportados como: vulnerabilidades, actualizaciones, parches de seguridad, etc.

3.2.2 Probabilidad.

Para definir la probabilidad de ocurrencia de que se materialice la amenaza se debe considerar lo siguiente:

No.	Escala	Descripción
1	Probabilidad Muy Baja	Los controles de seguridad existentes son seguros y eficaces.
2	Probabilidad Baja	Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.
3	Probabilidad Media	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Existe la posibilidad de que haya un incidente en el futuro.
4	Probabilidad Alta	Los controles de seguridad existentes son bajos o ineficientes. Existe una gran posibilidad de que haya incidentes así en el futuro.
5	Probabilidad Muy Alta	No existen controles de seguridad.

3.2.3 Degradación.

Para identificar el valor de la degradación que tendría el activo si la amenaza llegase a materializarse, se debe considerar la siguiente tabla:

No.	Escala	Descripción
1	Degradación Muy Baja	No existe un daño sobre el activo. [y ningún proceso crítico se vería afectado].
2	Degradación Baja	El daño derivado de la materialización de la amenaza degradaría al activo en lo más mínimo y no afectaría su valor. [afectación de un proceso no crítico].
3	Degradación Media	El daño derivado de la materialización de la amenaza degradaría al activo en una parte importante, y podría tener daños significativos en el valor del mismo. [afectación de varios procesos no críticos].
4	Degradación Alta	El daño derivado de la materialización de la amenaza degradaría al activo casi en su totalidad. [afectación de procesos críticos que pueden restablecerse en menos de dos días].
5	Degradación Muy Alta	El daño derivado de la materialización de la amenaza degradaría por completo al activo. y dejaría al activo inservible [afectación de procesos críticos que no pueden restablecerse en menos de dos días].

Nota: solo se deben seleccionar valores de 1, 2, 3, 4 y 5 todo valor fuera de estos rangos no permite obtener los resultados adecuados.

4. Evaluación del Riesgo Inherente.

4.1 Impacto Inherente.

Para obtener el valor del impacto se realiza a través de una multiplicación del activo por la degradación, como se representa en la siguiente fórmula:

Impacto Inherente = valor del activo * degradación inherente.

La fórmula utilizada es:

“Impacto Inherente =SI (I3*L3<4,1, SI (I3*L3<7,2, SI (I3*L3<10,3, SI(I3*L3<13,4,5)))”

Valor del impacto	Degradación				
Valor del activo	1	2	3	4	5
5	A	MA	MA	MA	MA
4	M	A	A	MA	MA
3	B	M	M	A	A
2	MB	B	B	M	M
1	MB	MB	MB	B	B

4.2 Riesgo Inherente.

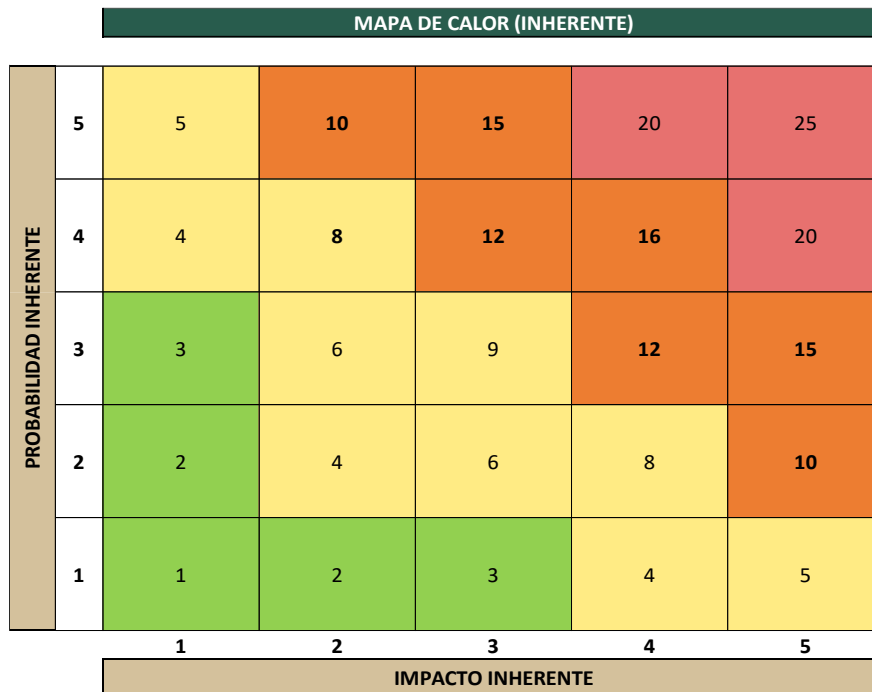
Para el cálculo del riesgo se obtiene multiplicando la probabilidad por el impacto como se observa en la fórmula;
Riesgo inherente = probabilidad inherente * impacto inherente.

La fórmula utilizada es:

“Riesgo Inherente =SI (K3*M3<4,"BAJO", SI (K3*M3<10,"MEDIO", SI (K3*M3<20,"ALTO","MUY ALTO"))))”

Descripción del riesgo	
Muy Alto	Nivel de riesgo crítico, se requiere tomar acciones inmediatas.
Alto	Se requiere tomar acciones planeadas.
Medio	Se sugiere aceptar el riesgo y realizar monitoreo de manera periódica.
Bajo	Se sugiere aceptar el riesgo y realizar monitoreo de manera periódica.

La siguiente matriz muestra el lugar donde se encuentra el riesgo.



 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

4.3 Ejemplo de Evaluación de Riesgo Residual.

Activo de Información	Descripción del Activo	Tipo de activo	Custodio	C	I	D	Valor del activo
Servidores productivos	Servidores del Instituto FONACOT que se encuentran en producción.	Aplicaciones (software)	Instituto FONACOT	5	5	5	5
Amenazas		Probabilidad	Degradación	Impacto		Valor del riesgo	
Desastres naturales (sismos).		3	5	5		ALTO	

4.4 Identificación de los Custodios de Riesgos.

Para cada riesgo es necesario identificar a la persona que es el custodio o unidad organizativa que tenga la responsabilidad y autoridad para gestionar los riesgos. Esta persona es la misma que el responsable del activo de información.

4.5 Tratamiento del Riesgo.

Proceso destinado a modificar el riesgo.

El tratamiento del riesgo puede implicar:

- Aceptar el riesgo.
- Evitar el riesgo.
- Mitigar el riesgo.
- Transferir el riesgo.

Identificación y elección de controles de seguridad.

5. INFORMES DE LOS RIESGOS.

El RSI documentará los resultados de la evaluación y tratamiento de riesgos y de todas las revisiones subsiguientes y presentará un informe con las actividades realizadas durante todo el proceso, además de presentar los controles elegidos para el tratamiento de los riesgos y en ese entendido se solicitarán los recursos humanos, técnicos y financieros necesarios para la implementación de estos.

Al firmar el “*Plan de Tratamiento de Riesgos*” queda por asentado la aprobación del RSI para la implementación y ejecución de los controles, y por ende la aprobación de todos los recursos necesarios para la gestión de este.

6. CRITERIOS PARA LA ACEPTACIÓN DEL RIESGO.

Los riesgos con valores de 5 y 4 deben ser tratados a la brevedad y deben tener un nivel de prioridad mayor sobre los otros riesgos, los riesgos con valor de 3 tienen prioridad media que deben resolverse en un lapso no mayor a 6 meses.

Cuando el nivel del riesgo sea un valor igual a 1 o 2, el Instituto FONACOT ha determinado que es un nivel aceptable para la organización y que solamente se va a requerir de monitorear constante el riesgo.

7. EVALUACIÓN DEL RIESGO RESIDUAL.

Las actividades para obtener el valor del riesgo residual son similares a la obtención del riesgo inherente.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

7.1 Evaluación del Riesgo Residual.

El proceso para la evaluación del riesgo residual es el siguiente:

- Validar la efectividad de los controles.
- Evaluar la probabilidad residual de ocurrencia.
- Evaluar la degradación residual de la amenaza.
- Se calcula el impacto residual (impacto residual = valor del activo * degradación residual).
- Se calcula el riesgo residual (riesgo = impacto residual * probabilidad residual).

7.2 Valoración de los Controles.

Para obtener el riesgo residual se evalúan los controles implementados o a implementar, tomando en cuenta la documentación del MGSI y las tecnologías de seguridad que estén implementadas a la fecha.

7.3 Probabilidad Residual.

Para evaluar la probabilidad residual se deben utilizar los mismos criterios que se encuentran en el apartado 4.2.2 de este documento.

Definir un valor a la probabilidad residual tomando en consideración la eficacia de los controles.

7.4 Degradación Residual.

Para obtener la degradación que tendría el activo se deben utilizar los mismos criterios que se encuentran en el apartado 4.2.3 de este documento.

Definir la magnitud de la degradación residual tomando en cuenta la eficacia de los controles.

7.5 Impacto Residual.

Dado un cierto conjunto de controles desplegados, y una medida de la madurez del proceso de gestión, el sistema queda en una situación de posible impacto que se denomina **Impacto Residual**. Se dice que hemos modificado el impacto, desde un valor inherente a un valor residual.

Repetir los cálculos de impacto con este nuevo nivel de degradación; **Impacto Residual = Valor del Activo * Degradación Residual**.

La fórmula utilizada es:

“Impacto Residual =SI (I3*T3<4,1, SI (I3*T3<7,2, SI (I3*T3<10,3, SI(I3*T3<13,4,5))))”

Nota: Esta fórmula solo es de referencia, ya que puede variar según las celdas y filas del libro donde se realice el análisis.

7.6 Riesgo Residual.

Dado un cierto conjunto de controles desplegados y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina **Riesgo Residual**. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

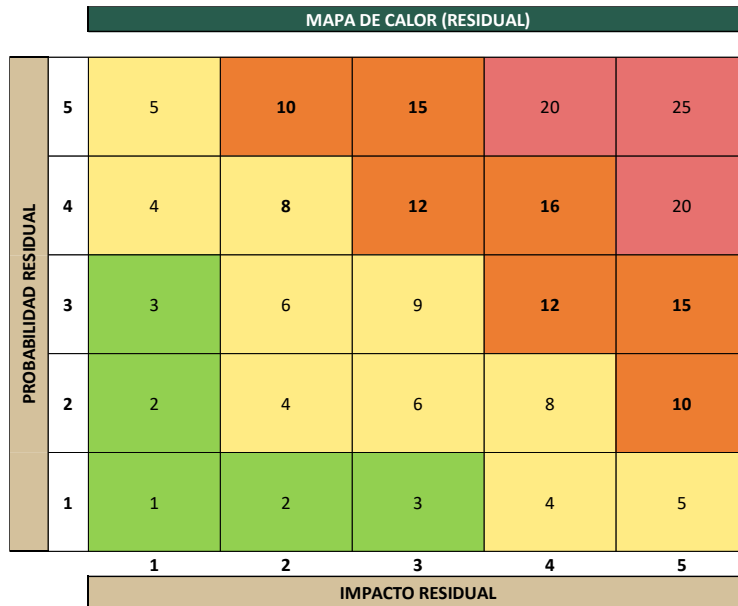
Repetir los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La fórmula utilizada para el riesgo residual es: **Riesgo Residual = (Impacto Residual * Probabilidad Residual)**.

La fórmula utilizada es:

“Riesgo Residual =SI (S3*U3<4,“ BAJO”, SI (S3*U3<10,“ MEDIO”, SI (S3*U3<20,“ ALTO”,“ MUY ALTO”))”

Nota: Esta fórmula solo es de referencia, ya que puede variar según las celdas y filas del libro donde se realice el análisis.



7.7 Ejemplo de Evaluación de Riesgo Residual.

RIESGO INHERENTE

Activo de Información	Descripción del Activo	Tipo de activo	Custodio	C	I	D	Valor del activo
Servidores productivos	Servidores del Instituto FONACOT que se encuentran en producción.	Aplicaciones (software)	Instituto FONACOT	5	5	5	5
Amenazas		Probabilidad	Degradación	Impacto		Valor del riesgo	
Desastres naturales (sismos).		3	5	5		ALTO	

TRATAMIENTO DEL RIESGO

Controles aplicables o de apoyo

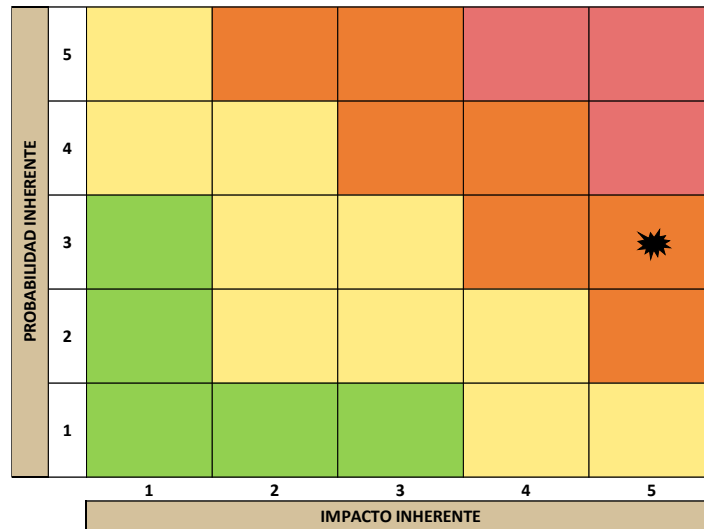
11.1.4 Protección contra amenazas externas y del ambiente, 11.1.1 Perímetro de seguridad físico, 11.2.1 Instalación y protección de equipo, 12.3.1 Respaldo de información, 17.2.1 Disponibilidad de instalaciones para el procesamiento de información.

RIESGO RESIDUAL

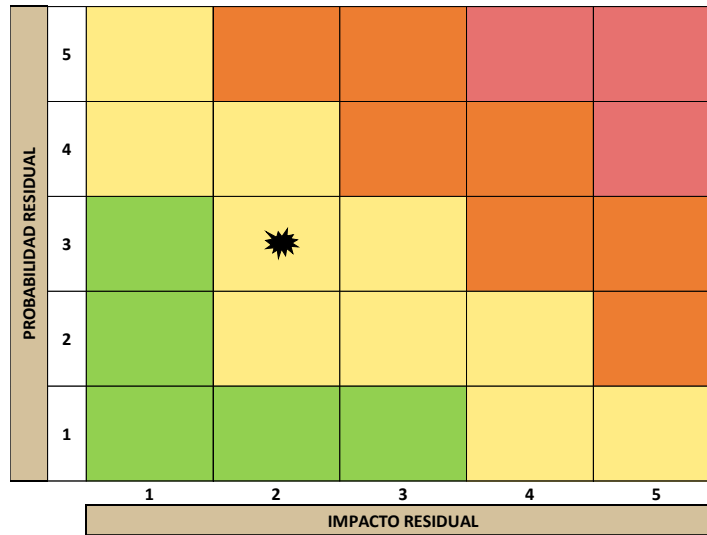
Probabilidad residual	Degradación residual	Impacto residual	Riesgo residual
3	1	2	MEDIO



MAPA DE CALOR (INHERENTE)



MAPA DE CALOR (RESIDUAL)



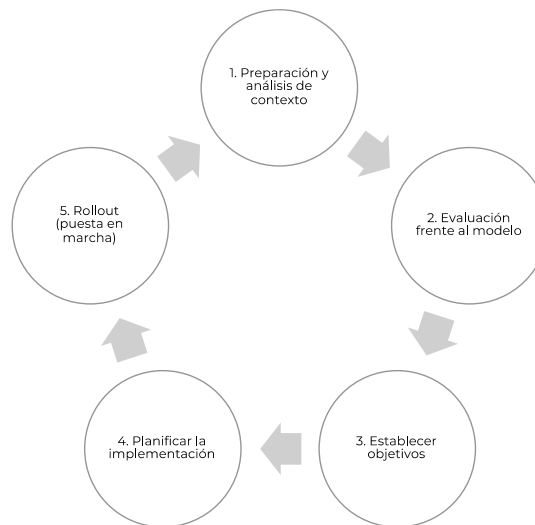
43. OWASP – SAMM INSTITUTO FONACOT.

1. INTRODUCCIÓN.

OWASP SAMM es el marco de trabajo para evaluar, formular e implementar estrategias para la seguridad del software, el cual se puede adoptar a cualquier tipo SDLC por implementar o ya existente.

El modelo se puede adoptar de forma transparente a desarrollo en cascada, iterativo, ágil y DevOps.

2. FRAMEWORK SAMM.



2.1 Preparación y Análisis de Contexto.

Propósito.

Asegurar inicio adecuado del proyecto.

Actividades:

- Definir el alcance – Establecer el objetivo del esfuerzo: todo el Instituto FONACOT, una aplicación o proyecto en particular, un equipo en particular.
- Identificar a los interesados - Asegurar que los interesados importantes estén identificados y alineados para apoyar el proyecto.
- Comunicar - Asegurar que las partes interesadas estén informadas.


2.2 Evaluación Frente al Modelo.

Propósito.

Identificar y comprender cada una de las actividades del plan de seguridad de software (*Ver sección – Plan de seguridad de Software*).

Actividades:

- Evaluar las actividades actuales – Organice entrevistas con las partes involucradas para comprender el estado actual de las actividades dentro del Instituto FONACOT.
- Determinar el nivel de madurez – En función del resultado, determinar para cada actividad de seguridad el nivel de madurez y determinar la brecha con relación al estado deseado.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

2.3 Establecer Objetivos.

Propósito.

Desarrollar un puntaje objetivo que se pueda usar para medir las actividades más importantes.

Actividades:

- Definir el objetivo – Establecer o actualizar el objetivo identificando qué actividades del Instituto FONACOT se debería implementar idealmente. Hay que asegurar que el conjunto total de actividades seleccionadas tenga sentido y dependencias entre actividades.
- Estimar el impacto general – Estimar el impacto del objetivo elegido en el Instituto FONACOT. Expresar en argumentos presupuestarios.

2.4 Planificar la Implementación.

Propósito.

Desarrollar o actualizar el plan para llevar al Instituto FONACOT al siguiente nivel respecto a la seguridad en el desarrollo de aplicaciones de software.

Actividades:

- Determinar el cronograma de cambios – Elegir una estrategia de cambio realista en términos de número y duración de fases. Una hoja de ruta típica consta de 4 a 6 fases durante 3 a 12 meses.
- Desarrollar / actualizar el plan de la hoja de ruta - Distribuir la implementación de actividades adicionales en las diferentes fases de la hoja de ruta, teniendo en cuenta el esfuerzo requerido para implementarlas. Equilibrar el esfuerzo de implementación en los diferentes períodos, teniendo en cuenta las dependencias entre actividades.

2.5 Implementación.

Propósito.

Administrar la planificación.

Actividades:

- Implementar actividades – Implementación de todas las actividades que forman parte del período. Considerar el impacto en los procesos, las personas, el conocimiento y las herramientas.

2.6 Rollout (puesta en marcha).

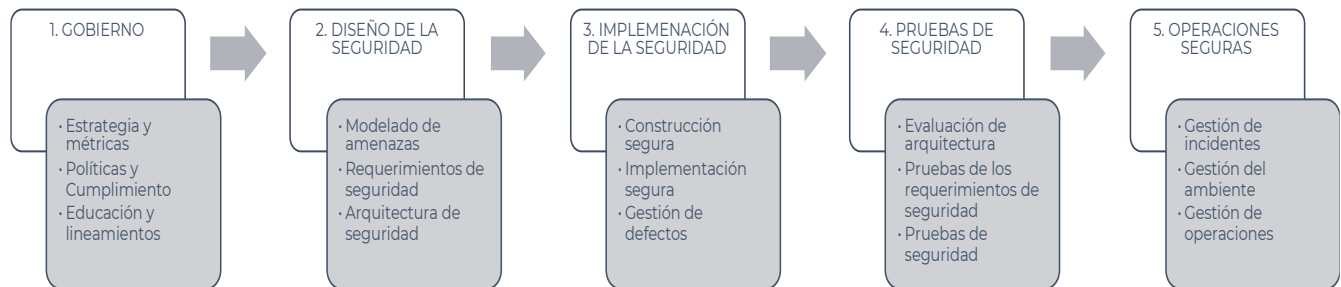
Propósito.

Asegurar que las mejoras en la seguridad para el proceso de desarrollo estén disponibles y se utilicen efectivamente dentro del Instituto FONACOT.

Actividades:

- Hacer que los pasos y las mejoras sean visibles para todos los involucrados mediante capacitación y sensibilización.
- Medir la adopción y la efectividad de las mejoras implementadas mediante el análisis del uso y el impacto.

3. PLAN DE SEGURIDAD DE SOFTWARE.



3.1 Gobierno.

- Estrategia y métricas.
 - Definir las métricas con información sobre la efectividad y la eficiencia del programa de seguridad de aplicaciones.
 - Establecer objetivos y KPI's para medir la efectividad del programa.
 - Estrategia basada en las métricas y las necesidades de la organización.
- Políticas y cumplimiento.
 - Identificar los controles y requisitos de cumplimiento indicados en políticas y estándares existentes.
 - Requisitos específicos de cumplimiento y guía de pruebas.
 - Medición y reporte del cumplimiento de los requisitos.
- Educación y lineamientos.
 - Ofrecer al personal laboral acceso a recursos en torno a los temas de desarrollo e implementación seguros.
 - Educar a todo el personal laboral en el ciclo de vida del software con tecnología y orientación específica de roles sobre desarrollo seguro.
 - Desarrollar programas de capacitación internos creados por los desarrolladores de los diferentes equipos involucrados en la solución.

3.2 Diseño de la Seguridad.

- Modelado de amenazas.
 - Realizar evaluación de riesgos de la aplicación para comprender la probabilidad y el impacto de un ataque.
 - Comprender el riesgo para todas las aplicaciones en la organización al centralizar el inventario de perfil de riesgo para las partes interesadas.
 - Revisión periódica de los perfiles de riesgo de la aplicación a intervalos regulares para garantizar la precisión y reflejar el estado actual.
- Requerimientos de seguridad.
 - Los objetivos de seguridad de aplicaciones de alto nivel se deben asignar a requerimientos funcionales.
 - Los requisitos de seguridad deben estar disponibles y ser utilizados por los equipos de desarrollo.
 - Desarrollar un marco de requisitos para que los equipos de desarrollo lo utilicen.
- Arquitectura de seguridad.
 - Consideraciones de seguridad en el proceso de diseño de software.
 - Proceso de diseño de software enfocado hacia servicios seguros.
 - Proceso de diseño de software y validación de la utilización de componentes seguros.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

3.3 Implementación de la Seguridad.

- a. Construcción segura.
 - i. Definición formal del proceso de compilación para que sea coherente y repetible.
 - ii. Identificar dependencias y prever reacciones oportunas a situaciones que supongan un riesgo a las aplicaciones.
 - iii. Comprobaciones de seguridad al proceso de compilación y prever que la creación de artefactos no falle.
- b. Implementación segura.
 - i. Formalizar el proceso de implementación y asegurar las herramientas y procesos utilizados.
 - ii. Automatizar el proceso de implementación en todas las etapas e introducir pruebas de verificación de seguridad.
 - iii. Verificar (con herramientas) la integridad de todo el software implementado.
- c. Gestión de defectos.
 - i. Seguimiento estructurado de defectos de seguridad y toma de decisiones informadas basadas en esta información.
 - ii. Evaluar todos los defectos de seguridad en toda la organización y definir los SLA.
 - iii. Aplicar los SLA definidos.

3.4 Pruebas de Seguridad.

- a. Evaluación de arquitectura.
 - i. Identificar los componentes de la arquitectura de aplicaciones e infraestructura y revisión del aprovisionamiento básico de seguridad.
 - ii. Validación de mecanismos de seguridad de la arquitectura.
 - iii. Revisión de la efectividad de los componentes de la arquitectura.
- b. Pruebas de los requerimientos de seguridad.
 - i. Análisis de vulnerabilidades periódicas y otros problemas de seguridad.
 - ii. Revisión de implementación para identificar los riesgos específicos de la aplicación respecto a los requisitos de seguridad.
 - iii. Mantener el nivel de seguridad de la aplicación después de la corrección de errores, cambios o durante el mantenimiento.
- c. Pruebas de seguridad (AST).
 - i. Realizar pruebas de seguridad para descubrir defectos de seguridad.
 - 1) Ejecución de SAST y DAST.
 - 2) Configuración de reglas, filtrado de falsos positivos.
 - 3) Automatización de procesos, tableros de control y los KPI.
 - ii. Realizar pruebas de penetración durante el desarrollo.
 - 1) Ejecución de pruebas de penetración Caja Negra (Black-box), Caja Blanca (White-box) y Caja Gris (Gray-box).
 - iii. Realizar pruebas de seguridad como parte de los procesos de desarrollo e implementación.
 - 1) Correlación de pruebas automatizadas y manuales.

3.5 Operaciones Seguras.

- a. Gestión de incidentes.
 - i. Utilizar los datos de registro disponibles para realizar la mejor detección de posibles incidentes de seguridad.
 - ii. Seguir el proceso establecido y documentado para la detección de incidentes, con énfasis en la evaluación automatizada de registros.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- iii. Utilizar el proceso de gestión de incidentes.
 - b. Gestión del ambiente.
 - i. Mejorar el hardening de las configuraciones.
 - ii. Realizar hardening de configuraciones.
 - iii. Monitoreo de las configuraciones y llevar a cabo la gestión de ocurrencias detectadas como defectos de seguridad.
 - a. Gestión de operaciones.
 - i. Implementación de mejores prácticas en la protección de datos.
 - ii. Desarrollo de catálogo de datos y establecer una política de protección de datos.
 - iii. Automatizar la detección de incumplimiento de políticas y auditar el cumplimiento periódico del catálogo de datos y de la política de protección de datos.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

44. METODOLOGÍA PARA EL ANÁLISIS CAUSA RAÍZ.

1. INTRODUCCIÓN.

El propósito de este documento es definir y establecer una metodología para identificar y analizar las causas que generan las no conformidades reales o potenciales que se presentan en los procesos o aplicaciones dentro del alcance del MGSÍ que hayan sido resultantes de las auditorías internas o externas.

2. ANÁLISIS CAUSA RAÍZ.

Es un método para el abordaje de no conformidades que intenta evitar la recurrencia de un inconveniente, problema, defecto o situación no deseada a través de identificar las causas que lo ocasionan.

Las causas están asociadas a uno o más factores como, por ejemplo:

- Mano de obra (personas/puestos).
- Máquinas y equipos (herramientas de soporte como: software, computadores, entre otros).
- Administración (administración o gestión de tipo administrativo que pueden ser decisiones o asignación de recursos).
- Método (metodología o mecanismo que usa el proceso como: modelos, planes, programas, fichas, listas, documentación, entre otros).
- Materiales (base usada para la actividad o proceso puede ser: información, productos, bienes y servicios, entre otros).
- Medio ambiente (infraestructura, ambiente de trabajo).
- Proveedores (incumplimiento en el servicio).
- Incidentes (afectaciones que perjudican a la operación).

A partir de estos factores, se realizan los cuestionamientos acerca de “¿por qué?” está ocurriendo esa situación, que debe controlarse o eliminarse. Realizado el análisis es necesario determinar las acciones correctivas o preventivas.

3. MÉTODO DE ANÁLISIS.

El método es la ruta o camino mediante el cual se llega a un fin. La ruta del mejoramiento es definida por el RSI, el cual permite al proceso y/o área ser más eficiente y eficaz, a partir de una toma de acciones coherentes, pertinentes y oportunas.

Existen diversas herramientas para realizar un análisis de causas y formular acciones a partir de él, a continuación, se describe la forma adoptada por el Instituto FONACOT.

3.1 Análisis Causa-Efecto o Espina de Pescado.

El Diagrama Causa-Efecto es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema.

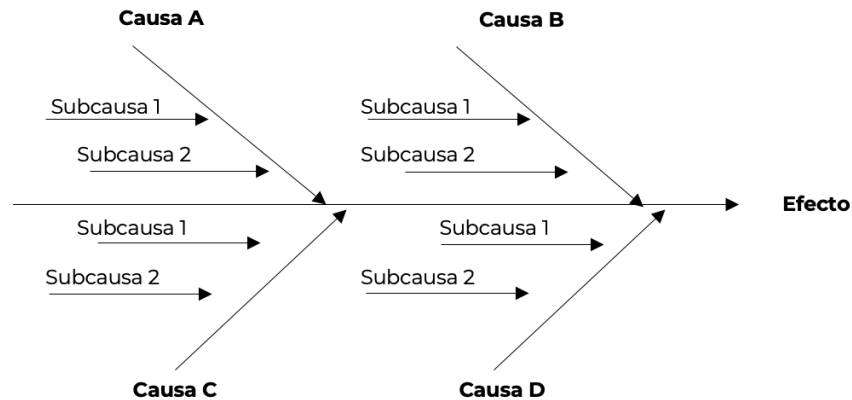
Es llamado usualmente Diagrama de “Ishikawa”, ya que su creador fue Kaoru Ishikawa, experto en dirección de empresas, interesado en mejorar el control de la calidad; también es llamado “Diagrama Espina de Pescado” porque su forma es similar al esqueleto de un pez.

Procedimiento.

- a) Identificar el problema: identifique y defina con exactitud el problema, fenómeno, evento o situación que se quiere analizar. Este debe plantearse de manera específica y correcta para que el análisis de las causas se oriente correctamente y se eviten confusiones.
- b) Identificar las principales categorías dentro de las cuales pueden clasificarse las causas del problema: se asume que todas las causas del problema que se identifiquen pueden clasificarse dentro de una u otra categoría.

- c) Identificar las causas: mediante una lluvia de ideas y teniendo en cuenta las categorías encontradas, identifique las causas del problema. Estas son por lo regular, aspectos específicos de cada una de las categorías que, al estar presentes de una u otra manera, generan el problema.
- d) Situar el efecto o característica a examinar en el lado derecho de lo que será el diagrama: en este debe aparecer, al menos, una breve descripción del efecto.
- e) Trazar una línea hacia la izquierda, partiendo del recuadro.
- f) Identificar las causas principales que inciden sobre el efecto: estas son las ramas principales del diagrama y constituyen las categorías bajo las cuales se relacionan otras posibles causas.
- g) Situar cada una de las categorías principales de causas en recuadros conectados con la línea central.
- h) Identificar, para cada rama principal, otros factores específicos que puedan ser causa del efecto: estos factores forman las ramas de segundo nivel. A su vez, estas pueden expandirse en otras de tercer nivel, y así sucesivamente. Para esta expansión recurrente, será útil emplear series de preguntas iniciadas con: “¿Por qué?” y verificar la inclusión de factores. Será preciso revisar el diagrama para asegurar que se han incluido todos los factores causales posibles.
- i) Analizar y discutir el diagrama: cuando el diagrama ya esté finalizado, el equipo de trabajo puede discutirlo, analizarlo y, si se requiere, realizarle modificaciones.

Ejemplo:



Consideraciones generales para elaborar y usar un diagrama causa-efecto.

- Identificar todos los factores relevantes mediante consulta y discusión entre las partes involucradas. Para ello, puede ser útil utilizar la “lluvia de ideas”.
- Expresar el efecto y los factores tan concretamente como sea posible, pues la abstracción lleva a obtener resultados útiles.
- Hacer un diagrama para cada característica, por ejemplo, si estudiamos los fallos en el grosor y en la longitud de una barra de acero, hacer un diagrama para el grosor y otra para la longitud.
- Asignar la importancia a cada factor objetivamente.
- Tratar de mejorar continuamente el diagrama de causa-efecto mientras es usado.

3.2 Los ¿Por qué?

Es una técnica sistemática de preguntas utilizadas en la fase de análisis de problemas para buscar posibles causas principales de un problema. La técnica requiere que el equipo pregunte “¿por qué?” al menos tres veces.

¿Cómo se utiliza?

- Realizar una sesión de lluvia de ideas.
- Una vez que la causa más probable haya sido identificada, se debe empezar a preguntar “¿Por qué es así?” o “¿Por qué está pasando esto?”.
- Continuar preguntado “¿por qué?” al menos 3 veces. Esto reta al equipo a buscar a fondo y no conformarse con causas ya “probadas y ciertas”.
- Durante este tiempo se debe tener cuidado de NO empezar a preguntar “Quién”. Se debe recordar que el equipo está interesado en el proceso y no en el personal laboral involucrado.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

45. OWASP VERIFICACIÓN DE SEGURIDAD EN APLICACIONES MÓVILES.

1. INTRODUCCIÓN.

El MASVS se utiliza para establecer un nivel de confianza en la seguridad de las aplicaciones móviles.

- Uso como una métrica – Proporciona un estándar dirigido tanto a desarrolladores como a los responsables de aplicaciones, el cual puede ser utilizado para comparar aplicaciones en términos de seguridad.
- Uso como guía – Hace de guía durante todas las fases del desarrollo y pruebas de seguridad de las aplicaciones móviles.
- Uso durante la compra o contratación – Proporcionar una línea base para la verificación de la seguridad de aplicaciones móviles.

2. REQUERIMIENTOS DE ARQUITECTURA, DISEÑO Y MODELADO.

Objetivo.

Planificar la arquitectura de la aplicación móvil, conocer los roles funcionales y de seguridad de todos los componentes.

Verificación de Seguridad.

- **MSTG-ARCH-1:** Todos los componentes se deben identificar y de asegurar que son necesarios.
- **MSTG-ARCH-2:** Los controles de seguridad nunca se deben aplicar sólo en el cliente, sino que también en los respectivos servidores.
- **MSTG-ARCH-3:** Se debe definir una arquitectura de alto nivel para la aplicación y los servicios.
- **MSTG-ARCH-4:** Se debe identificar claramente la información considerada sensible en el contexto de la aplicación móvil.
- **MSTG-ARCH-5:** Todos los componentes de la aplicación deben estar definidos en términos de la lógica de negocio o las funciones de seguridad que proveen.
- **MSTG-ARCH-6:** Se debe realizar un modelado de amenazas para la aplicación móvil y los servicios en el que se definieron las mismas y sus contramedidas.
- **MSTG-ARCH-7:** Todos los controles de seguridad deben tener una implementación centralizada.
- **MSTG-ARCH-8:** Debe existir una política explícita sobre el uso de claves criptográficas (si se usan) a través de todo su ciclo de vida.
- **MSTG-ARCH-9:** Debe existir un mecanismo para forzar las actualizaciones de la aplicación móvil.
- **MSTG-ARCH-10:** La implementación de medidas de seguridad debe ser una parte esencial durante todo el ciclo de vida del desarrollo de software de la aplicación.
- **MSTG-ARCH-11:** Debe existir una política de divulgación responsable y debe ser llevada a cabo adecuadamente.
- **MSTG-ARCH-12:** La aplicación debe cumplir con las leyes y regulaciones de privacidad.

3. REQUERIMIENTOS DE ALMACENAMIENTO DE DATOS Y PRIVACIDAD.

Objetivo.

Proteger los datos sensibles, como las credenciales del personal y la información privada, ya que esto es un aspecto clave en la seguridad de la información en las aplicaciones móviles. Se considera que los datos confidenciales pueden exponerse involuntariamente a otras aplicaciones que se ejecutan en el mismo dispositivo o bien filtrarse involuntariamente en el almacenamiento en la nube, copias de seguridad o el caché del teclado. Otro escenario es el extravío o robo de los dispositivos, por lo que es muy probable que un atacante busque tener acceso al mismo, bajo este escenario es necesario implementar protecciones para dificultar la recuperación de los datos sensibles.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Verificación de Seguridad.

- **MSTG-STORAGE-1:** Las funcionalidades de almacenamiento de credenciales del sistema deben ser utilizadas para almacenar información sensible, tal como información personal, credenciales o claves criptográficas.
- **MSTG-STORAGE-2:** No se debe almacenar información sensible fuera del contenedor de la aplicación o del almacenamiento de credenciales del sistema.
- **MSTG-STORAGE-3:** No debe escribir información sensible en los registros (logs) de la aplicación.
- **MSTG-STORAGE-4:** No se debe compartir información sensible con servicios externos, salvo que sea una necesidad de la arquitectura.
- **MSTG-STORAGE-5:** Se debe desactivar el caché del teclado en los campos de texto que contienen información sensible.
- **MSTG-STORAGE-6:** No se debe exponer información sensible mediante mecanismos de comunicación entre procesos (IPC).
- **MSTG-STORAGE-7:** No se debe exponer información sensible como contraseñas y números de tarjetas de crédito a través de la interfaz o capturas de pantalla.
- **MSTG-STORAGE-8:** No se debe incluir información sensible en las copias de seguridad generadas por el sistema operativo.
- **MSTG-STORAGE-9:** La aplicación eliminará toda información sensible de la vista cuando la aplicación pasa a un segundo plano.
- **MSTG-STORAGE-10:** La aplicación no conservará ninguna información sensible en memoria más de lo necesario y la memoria se debe limpiar tras su uso.
- **MSTG-STORAGE-11:** La aplicación obligará a que exista una política mínima de seguridad en el dispositivo, como la necesidad de configurar un código de acceso.
- **MSTG-STORAGE-12:** La aplicación indicará los tipos de información personal que procesa y de las mejores prácticas en seguridad que se deben seguir al utilizar la aplicación.
- **MSTG-STORAGE-13:** No se debe guardar ningún tipo de información sensible de forma local en el dispositivo móvil. En su lugar, esa información debe ser obtenida desde un sistema remoto sólo cuando es necesario y únicamente residir en memoria.
- **MSTG-STORAGE-14:** En caso de ser necesario almacenar información sensible de forma local, esta debe ser cifrada usando una clave derivada del hardware de almacenamiento seguro, el cual debe requerir autenticación previa.
- **MSTG-STORAGE-15:** El almacenamiento local de la aplicación debe ser borrado tras un número excesivo de intentos fallidos de autenticación.

4. REQUERIMIENTOS DE CRIPTOGRAFÍA.

Objetivo.

Asegurar que la aplicación móvil utiliza criptografía siguiendo las mejores prácticas de la industria, incluyendo:

- Uso de librerías criptográficas reconocidas y probadas.
- Configuración y elección apropiada de primitivas criptográficas.
- Uso de generadores de números aleatorios suficientemente seguros.

Verificación de Seguridad.

- **MSTG-CRYPTO-1:** La aplicación no debe depender únicamente de criptografía simétrica cuyas claves se encuentran directamente en el código fuente de la misma.
- **MSTG-CRYPTO-2:** La aplicación debe utilizar implementaciones de criptografía probadas.
- **MSTG-CRYPTO-3:** La aplicación debe utilizar claves de seguridad que son apropiadas para el caso particular y su configuración y parámetros siguiendo las mejores prácticas de la industria.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- **MSTG-CRYPTO-4:** La aplicación no utilizará protocolos o algoritmos criptográficos considerados obsoletos para su uso en seguridad.
- **MSTG-CRYPTO-5:** La aplicación no debe reutilizar una misma clave criptográfica para varios propósitos.
- **MSTG-CRYPTO-6:** Los valores aleatorios deben ser generados utilizando un generador de números aleatorios seguro.

5. REQUERIMIENTOS DE AUTENTICACIÓN Y MANEJO DE SESIONES.

Objetivo.

Definir los requerimientos básicos sobre la gestión de cuentas y sesiones.

Verificación de Seguridad.

- **MSTG-AUTH-1:** Si la aplicación provee acceso a un servicio remoto, se debe contar con un mecanismo de autenticación ejecutado en el servidor remoto.
- **MSTG-AUTH-2:** Si se utiliza la gestión de sesión por estado, el servidor remoto debe usar tokens de acceso aleatorio para autenticar las solicitudes del cliente sin requerir el envío de las credenciales en cada petición.
- **MSTG-AUTH-3:** Si se utiliza la autenticación basada en tokens sin estado, el servidor debe proporcionar un token que se ha firmado utilizando un algoritmo seguro.
- **MSTG-AUTH-4:** Cuando se cierra la sesión en el dispositivo, se debe terminar la sesión también en el servidor.
- **MSTG-AUTH-5:** Debe existir una política de contraseñas aplicada en el servidor.
- **MSTG-AUTH-6:** El servidor debe tener mecanismos de seguridad para controlar que las credenciales de autenticación no sean ingresadas en una cantidad excesiva de veces.
- **MSTG-AUTH-7:** Las sesiones y los tokens de acceso deben expirar luego de un tiempo predefinido de inactividad.
- **MSTG-AUTH-8:** La autenticación biométrica, si la hay, no debe estar asociada a eventos (p. ej. usando una API que simplemente retorna "true" o "false"), sino basada en el desbloqueo del keychain/keystore (almacenamiento seguro).
- **MSTG-AUTH-9:** El sistema remoto debe tener implementado un mecanismo de segundo factor de autenticación (2FA).
- **MSTG-AUTH-10:** Para realizar transacciones críticas se debe requerir una autenticación adicional (step-up).
- **MSTG-AUTH-11:** La aplicación debe informar acerca de todas las actividades sensibles en la cuenta. Se debe tener la posibilidad de ver una lista de los dispositivos conectados, información contextual (dirección IP, localización, etc.), y tener la capacidad de bloquear los dispositivos.
- **MSTG-AUTH-12:** Los modelos de autorización deben ser definidos y ejecutados por el sistema remoto.

6. REQUERIMIENTOS DE COMUNICACIÓN A TRAVÉS DE LA RED.

Objetivo.

Asegurar la confidencialidad e integridad de la información que es intercambiada entre la aplicación móvil y los servicios del servidor. Utilizar canales seguros y cifrados utilizando el protocolo TLS con las configuraciones apropiadas.

Verificación de Seguridad.

- **MSTG-NETWORK-1:** La información debe ser enviada de manera cifrada utilizando TLS. El canal seguro debe ser usado de manera consistente en la aplicación.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- **MSTG-NETWORK-2:** Las configuraciones del protocolo TLS deben basarse en las mejores prácticas de la industria, o hacer lo mejor posible en caso de que el sistema operativo del dispositivo no soporte los estándares recomendados.
- **MSTG-NETWORK-3:** La aplicación debe verificar el certificado X.509 del sistema remoto al establecer el canal seguro y sólo se deben aceptar certificados firmados por una CA de confianza.
- **MSTG-NETWORK-4:** La aplicación debe utilizar su propio almacén de certificados o realiza pinning del certificado o la clave pública del servidor. Bajo ningún concepto debe establecer conexiones con servidores que ofrecen otros certificados o claves, incluso si están firmados por una CA de confianza.
- **MSTG-NETWORK-5:** La aplicación no debe depender de un canal de comunicaciones inseguro (email o SMS) para operaciones críticas como registros personales o recuperación de cuentas.
- **MSTG-NETWORK-6:** La aplicación debe utilizar bibliotecas de conectividad y seguridad actualizadas.

7. REQUERIMIENTOS DE INTERACCIÓN CON LA PLATAFORMA.

Objetivo.

Utilizar las API de la plataforma y componente estándar de una manera segura, así como la comunicación entre aplicaciones (IPC).

Verificación de Seguridad.

- **MSTG-PLATFORM-1:** La aplicación solamente debe utilizar los permisos mínimos necesarios.
- **MSTG-PLATFORM-2:** Todo dato ingresado por cualquier medio debe ser validado. Esto incluye información recibida de manera personal, por la UI o mecanismos IPC como los Intentos, las URL y datos provenientes de la red.
- **MSTG-PLATFORM-3:** La aplicación no debe exponer ninguna funcionalidad sensible a través esquemas de URL salvo que dichos mecanismos estén debidamente protegidos.
- **MSTG-PLATFORM-4:** La aplicación no debe exponer ninguna funcionalidad sensible a través de mecanismos IPC salvo que dichos mecanismos estén debidamente protegidos.
- **MSTG-PLATFORM-5:** JavaScript se debe deshabilitar en los WebViews salvo que sea necesario.
- **MSTG-PLATFORM-6:** Las WebViews se deben configurar para permitir el mínimo de esquemas (idealmente, sólo https). Esquemas peligrosos como file, tel y app-id deben deshabilitarse.
- **MSTG-PLATFORM-7:** Si los objetos nativos son expuestos en WebViews, se debe verificar que cualquier componente JavaScript se cargue exclusivamente desde el contenedor de la aplicación.
- **MSTG-PLATFORM-8:** La serialización de objetos, si se realiza, se debe implementar utilizando API seguras.
- **MSTG-PLATFORM-9:** La aplicación se debe proteger contra ataques de tipo screen overlay. (sólo Android)
- **MSTG-PLATFORM-10:** La caché, el almacenamiento y los recursos cargados (JavaScript, etc.) de las WebViews deben ser borrados antes de destruir la WebView.
- **MSTG-PLATFORM-11:** Se debe verificar que la aplicación impida el uso de teclados de terceros siempre que se introduzca información sensible.

8. REQUERIMIENTOS DE CALIDAD DE CÓDIGO Y CONFIGURACIÓN DEL COMPILADOR.

Objetivo.

Asegurar las prácticas de seguridad en el desarrollo de la aplicación.

Verificación de Seguridad.

- **MSTG-CODE-1:** La aplicación debe ser firmada y provista con un certificado válido, cuya clave privada debe estar protegida.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

- **MSTG-CODE-2:** La aplicación debe ser publicada en modo release y con las configuraciones apropiadas para el mismo (por ejemplo, non-debuggable).
- **MSTG-CODE-3:** Los símbolos de depuración deben ser eliminados de los binarios nativos.
- **MSTG-CODE-4:** Cualquier código de depuración y/o de asistencia al desarrollador (p. ej. código de test, backdoors, configuraciones ocultas) deben ser eliminados. La aplicación no debe crear logs detallados de errores ni de mensajes de depuración.
- **MSTG-CODE-5:** Todos los componentes de terceros se deben tener identificados y revisados en cuanto a vulnerabilidades conocidas.
- **MSTG-CODE-6:** La aplicación debe capturar y gestionar debidamente las posibles excepciones.
- **MSTG-CODE-7:** Los controles de seguridad deben negar el acceso por defecto.
- **MSTG-CODE-8:** El código debe gestionar la memoria solicitada, utilizada y liberada de manera correcta.
- **MSTG-CODE-9:** Las funcionalidades de seguridad gratuitas de las herramientas, tales como minificación del byte-code, protección de la pila, soporte PIE y conteo automático de referencias, deben estar activadas.

9. REQUERIMIENTOS DE RESISTENCIA ANTE LA INGENIERÍA INVERSA.

Objetivo.

Seguridad para aplicaciones móviles que maneja o brindan acceso a información o funcionalidades sensibles, a través del incremento de la resistencia contra la ingeniería inversa de la aplicación, dificultando al atacante el acceso a los datos o el entendimiento del modo de ejecución de la aplicación.

Verificación de Seguridad.

Impedir el Análisis Dinámico y la Manipulación.

- **MSTG-RESILIENCE-1:** La aplicación debe detectar la utilización de un dispositivo rooteado, se debe notificar y finalizar la ejecución de la aplicación.
- **MSTG-RESILIENCE-2:** La aplicación debe considerar todos los protocolos de depuración.
- **MSTG-RESILIENCE-3:** La aplicación debe detectar y reportar cualquier modificación de ejecutables y datos críticos de la propia aplicación.
- **MSTG-RESILIENCE-4:** La aplicación debe detectar la presencia de herramientas de ingeniería inversa o frameworks.
- **MSTG-RESILIENCE-5:** La aplicación debe detectar y reportar cuando sea ejecutada en un emulador.
- **MSTG-RESILIENCE-6:** La aplicación debe detectar y reportar modificaciones de código o datos en su propio espacio de memoria.
- **MSTG-RESILIENCE-7:** La aplicación debe contar con múltiples mecanismos de detección para los puntos del 8.1 al 8.6.
- **MSTG-RESILIENCE-8:** Los mecanismos de detección debe considerar diferentes tipos de respuestas, incluyendo respuestas retardadas y silenciosas.
- **MSTG-RESILIENCE-9:** La ofuscación debe aplicarse en las defensas del programa, lo que a su vez impedirá la desofuscación mediante análisis dinámico.

Asociación del Dispositivo

- **MSTG-RESILIENCE-10:** La aplicación debe contar con un “enlace al dispositivo” utilizando una huella del dispositivo generada de varias propiedades únicas del mismo. La finalidad es impedir la Comprensión.
- Impedir la Comprensión.
- **MSTG-RESILIENCE-11:** Todos los archivos ejecutables y bibliotecas correspondientes a la aplicación se deben cifrar, los segmentos importantes de código deben estar cifrados o “empaquetados” (packed). De modo que cualquier análisis estático no revele código o datos importantes.
- **MSTG-RESILIENCE-12:** Debe utilizarse un esquema de ofuscación contra métodos de desofuscación manual y automatizada. La eficacia del esquema de ofuscación debe verificarse mediante pruebas manuales.

	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Impedir la Escucha (eavesdropping).

- **MSTG-RESILIENCE-13:** A modo de defensa en profundidad, además de incluirse un hardening de la comunicación, se debe considerar la implementación de un cifrado de datos (payloads) a nivel de aplicación como medida adicional contra ataques de Escucha (eavesdropping).

XVII. GLOSARIO DE TÉRMINOS.

1 DEFINICIONES.

Para efectos del presente Marco, se entenderá por:

Concepto	Definición
Acceso Privilegiado:	Acceso que permite a una persona realizar acciones que pueden modificar los sistemas, la comunicación de red, cuentas, archivos, datos o procesos. El acceso privilegiado generalmente se otorga a los administradores del sistema, de red, de infraestructura u otras personas cuyas tareas laborales requieren acceso a datos confidenciales que residen en un sistema, aplicativo o red. Estos datos pueden ser en papel o medios digitales. A los efectos de esta política, las cuentas de acceso a aplicaciones y otros desarrollos también se consideran privilegiados.
Acción Correctiva:	Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.
Aceptación de Riesgo:	Decisión informada de tomar un riesgo particular.
Activos:	Es cualquier recurso o competencia, los activos pueden ser de alguno de los siguientes tipos: gestión, organización, procesos, conocimientos, personas, información, aplicaciones, infraestructura o el capital financiero.
Adaptador Bluetooth USB:	Dispositivo a través del cual se puede compartir información con otros dispositivos.
Administrador/Root:	Cuentas con privilegios para realizar acciones superiores a los de una cuenta normal en equipos tecnológicos.
Algoritmo de Cifrado:	Es un componente para la seguridad del transporte electrónico de datos, donde se pueden utilizar diferentes tipos de cifrados para cifrar la información.
Amenaza:	Potencial causa de un incidente no deseado, que puede resultar en daño a un sistema u organización.
Análisis de Riesgo:	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Application Security Testing:	Prueba de seguridad de aplicaciones.
Auditado:	Es la persona u organización por auditar.
Auditor(a):	Persona con la competencia para llevar a cabo una auditoría.
Auditoría:	Proceso sistemático, independiente y documentado para obtener evidencias del funcionamiento e implantación del MGSI y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios establecidos por disposiciones planificadas, requisitos de la norma y requisitos del mismo sistema.
Backdoor:	Puerta trasera. Programa malicioso de ordenador usado para proporcionar al atacante un acceso remoto al equipo comprometido explotando vulnerabilidades del sistema.
Base de Datos:	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
Borrado de Datos:	Principio de seguridad de la información que consiste en asegurar que el acceso al activo únicamente se realiza por los autorizados y a través de los procedimientos establecidos para ello.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Concepto	Definición
Borrado Seguro:	Son servicios que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura según la normativa vigente.
Certificado X.509:	Es un certificado digital que utiliza el estándar internacional de infraestructura de clave pública (PKI) X.509 ampliamente aceptado para verificar que una clave pública pertenece a la identidad de quien lo usa, dispositivo o servicio contenida en el certificado.
Ciclo de Deming:	Es el Ciclo de Mejor Continua Deming (Planear, Hacer, Verificar y Actuar), el cual no se ejecuta una vez, sino que es continuo que busca mejorar procesos e iteraciones.
Cifrado:	Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje entendible a un mensaje incomprensible o difícil de comprender a toda persona que no tenga la clave secreta.
Clave Criptográfica:	Es una pieza de información que controla la operación de un algoritmo de cifrado, habitualmente siendo una secuencia de números o letras mediante la cual permite realizar el cifrado de la información.
Componentes:	Se constituye por los sistemas operativos, equipos de comunicación y equipos de seguridad.
Comunicación entre Procesos:	Es un método mediante el cual un proceso se comunica con otro a través del kernel del dispositivo para coordinar sus actividades.
Comunicación y Consulta:	Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas, relacionadas con la gestión del riesgo.
Concentrador VPN:	Dispositivo de red que provee la creación segura de conexiones VPN.
Confidencialidad:	Es un principio de seguridad que requiere que solo las personas autorizadas puedan tener acceso a los datos.
Conformidad:	Es el cumplimiento de un requisito en el MGSi.
Contraseña:	Clave que brinda un acceso, es única e intransferible.
Control:	Es una medida que modifica el riesgo, entre los cuales pueden ser un proceso, una política, tecnologías u otras acciones.
Control de Acceso:	El control de acceso ayuda a proteger la confidencialidad, integridad y disponibilidad de los activos, garantizando que sólo la persona y cuenta autorizada puede accederlos o modificarlos.
CREDERE:	<p>Sistema de control de operaciones crediticias para la originación y administración del crédito FONACOT.</p> <p>El sistema CREDERE enlaza en tiempo real a todas las oficinas del Instituto FONACOT a nivel nacional (DEPyR, y Oficinas Centrales).</p>
Criterios de Riesgo:	Términos de referencia contra los cuales se evalúa la importancia del riesgo.
Cuenta de Aplicativo:	Cuenta usada para la configuración, sincronización, migración o funcionamiento de un aplicativo que cuenta con derechos administrativos.
Cuenta de Servicio:	Cuenta usada para la configuración, sincronización, migración o funcionamiento de un servidor que cuenta con derechos administrativos.
Cuenta Privilegiada:	Acceso que permite a una persona realizar acciones que pueden modificar los sistemas, la comunicación de red, cuentas, archivos, datos o procesos. El acceso privilegiado generalmente se otorga a los administradores del sistema, de red, de

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	



Concepto	Definición
	infraestructura u otras personas cuyas tareas laborales requieren acceso a datos confidenciales que residen en un sistema, aplicativo o red. Estos datos pueden ser en papel o medios digitales. A los efectos de esta política, las cuentas de acceso a aplicaciones y otros desarrollos también se consideran privilegiados.
Custodios de los Activos de Información:	Todo aquel servidor público, mujer u hombre laborando en el Instituto FONACOT, que realce la gestión de los activos de información pertenecientes al Instituto FONACOT.
Database Management System:	Es una colección de software muy específico, orientado al manejo de base de datos, cuya función es servir de interfaz entre la base de datos, el personal autorizado y las distintas aplicaciones empleadas.
Degradación:	Es el nivel de afectación sobre el activo ante cualquier amenaza.
Destrucción Documental:	Son servicios destinados a la destrucción de datos confidenciales y documentos, con el fin de evitar sanciones administrativas por incumplimiento con la legislación.
Diagrama de Ishikawa:	Es una herramienta de la calidad que ayuda a levantar las causas-raíces de un problema, analizando todos los factores que involucran la ejecución del proceso.
Disponibilidad:	Es la habilidad de un servicio de TI u otro elemento de configuración para realizar la función acordada cuando sea requerido.
Dispositivo Móvil:	Dispositivo informático que tiene capacidades de comunicación bidireccional a través de diversos canales y protocolos, procesamiento y almacenamiento de datos. Con dimensiones y peso adecuado para que sea portado y/o trasladado por una persona de un punto a otro sin la necesidad de un medio de transporte.
Documento Obsoleto:	Es aquel que derivado de un cambio o emisión pierde su vigencia.
Equipo de Cómputo:	Las computadoras, equipos de uso personal y sus periféricos, considerando como equipo de cómputo de escritorio (desktop): el gabinete que contiene la Unidad Central de Proceso "CPU", el monitor, el teclado, el ratón (mouse) y cualquier otro equipo electrónico que transmita, ingrese o extraiga información del "CPU" (incluye memoria RAM, tarjetas de video, etc.), y a las computadoras portátiles o "laptop" como la unidad en sí misma.
Equipos de Comunicación:	Hardware utilizado para las soluciones de comunicación.
Equipo de Respuesta de Incidentes de Seguridad y Controles:	Grupo conformado por la SSOS y por el RSI.
Equipos de Seguridad:	Hardware utilizado para la protección de la confidencialidad e integridad en los contenedores de la información.
Estándar de Verificación de Seguridad de Aplicaciones Móviles:	Es una estándar para establecer un nivel de confianza en la seguridad de las aplicaciones móviles., es decir, establece un marco de requisitos de seguridad necesarios para diseñar, desarrollar y probar aplicaciones móviles seguras en iOS y Android.
Evaluación de Riesgos:	Proceso general de identificación de riesgos, análisis de riesgos y valoración de riesgos.
Evidencia Objetiva:	Es la información que puede ser aprobada como verdadera, basada en hechos obtenidos por medio de observación, medición, prueba u otros medios.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Concepto	Definición
Gestión de Incidentes de Seguridad de la Información:	Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información.
Grupo de Seguridad de la Información:	Equipo conformado por la DTI, DIT, SDSI, SSOS y por el RSI.
Hardening:	Palabra en inglés que significa endurecimiento. Proceso de asegurar un equipo de cómputo mediante la reducción de vulnerabilidades modificando su configuración.
Hardware:	Al conjunto de componentes físicos electrónicos que procesa y/o transmite datos y que forman parte de la infraestructura tecnológica del Instituto FONACOT.
Herramientas de Borrado Seguro:	Son herramientas que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura.
Herramientas de Destrucción Documental:	Son herramientas destinadas a la destrucción de datos confidenciales y documentos.
Impacto:	Es una medida del efecto de un incidente, problema o cambio en los procesos de negocio. A menudo, el impacto se establece en función de cómo los niveles de servicio se ven afectados. El impacto inherente hace referencia a la evaluación del riesgo sin contemplar los controles implementados.
Información Confidencial:	Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.
Información Documentada:	Información que se requiere ser controlada y mantenida y el medio en donde es contenida, se puede referir a: a. El sistema de gestión, incluyendo sus procesos relacionados. b. La información creada con el objetivo de que el Instituto FONACOT opere (documentación).
Infraestructura como Servicio:	Servicios de oferta de computación en la nube en la que un proveedor proporciona acceso a recursos informáticos, tales como: Servidores, Almacenamiento y redes.
Infraestructura Tecnológica:	Conjunto de recursos de telecomunicaciones, hardware y software que permitan el procesamiento, la transmisión y el almacenamiento de datos, audio o video.
Instituto del Fondo Nacional para el Consumo de los Trabajadores:	Organismo público descentralizado de interés social, con personalidad jurídica y patrimonio propio, así como con autosuficiencia presupuestal y sectorizado en la Secretaría del Trabajo y Previsión Social.
Integridad:	Es un principio de seguridad que garantiza que los datos y elementos de configuración solo puedan ser modificados por personas y actividades autorizadas.
Licencia:	Permiso legal otorgado por un tercero con facultades para ello, para utilizar un producto, generalmente software, a cambio de un pago único o periódico.
Lista Maestra de Información Documentada:	Documento que integra los nombres de los documentos y registros del Sistema de Gestión de Seguridad de la Información y dónde se define su control.
Lluvia de Ideas:	Es una herramienta de trabajo grupal que facilita el surgimiento de nuevas ideas sobre un tema o problema determinado.
Malware:	Malware o software malicioso es un término que se utiliza para hablar de todo tipo de amenazas informáticas o software hostil, entre ellas están los: virus, gusanos, troyanos, keyloggers, botnets, spyware, adware, ransomware y scareware.
Mantenimiento Correctivo:	La reparación de equipos que presentan alguna falla en su operación.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Concepto	Definición
Mantenimiento Preventivo:	Actividades de revisión y reacondicionamiento de equipos en forma programada, para prevenir fallas en la operación de estos.
Medio de Almacenamiento Externo Removible:	Componente informático independiente, específicamente diseñado para el almacenamiento de archivos que pueden ser de texto, de imagen, de sonido, de vídeo, programas informáticos, etc. Ejemplos de dispositivos de almacenamiento extraíbles son los siguientes: <ul style="list-style-type: none"> • Memoria USB. • Disco Duro Portátil. • Tarjeta de Memoria. • CD-RW. • DVD.
Mejora:	Acción tomada cuando se identifica que se puede para aumentar la capacidad del MGSÍ. El no llevar a cabo dichas actividades no representa un riesgo de No Conformidad a los requisitos del MGSÍ.
Marco de Gestión de Seguridad de la Información:	Es el conjunto de políticas, procedimientos y recursos que adoptan las instituciones de la APF para fortalecer la seguridad de la información; incluye la clasificación de activos de información institucionales, el análisis de riesgos, gestión de vulnerabilidades, respuesta a incidentes, planes de continuidad y supervisión y Mejora Continua.
Modelado de Amenazas:	Una técnica que consiste en desarrollar arquitecturas de seguridad cada vez más perfeccionadas para identificar agentes de amenazas, zonas de seguridad, controles de seguridad e importantes activos.
No Conformidad:	Incumplimiento a un requisito del MGSÍ.
Plataforma as a Service:	Servicio en la nube en la cual el proveedor proporciona al cliente un entorno de donde se pueda desarrollar y ofrecer aplicaciones.
Pandemia:	Afectación de una enfermedad infecciosa de los humanos a lo largo de un área geográficamente extensa.
Parche de Seguridad:	Un parche es una acumulación de correcciones para un posible problema o problema conocido del sistema operativo.
Periféricos:	Elementos electrónicos de entrada y/o salida de información, que pueden ser conectados a un equipo de cómputo. Son periféricos: impresoras, scanners, webcams, multifuncionales, proyectores, pizarrones interactivos, ploters y artículos similares.
Persona Auditora Líder:	Persona con capacidad para extraer información, analizar esa información e informar de los resultados de manera comprensible.
Personal Laboral:	Todo aquel recurso que forma parte de la fuerza laboral del Instituto FONACOT, que utiliza la red, los equipos y/o periféricos, propiedad del Instituto FONACOT.
Phishing:	Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza, haciéndose pasar por una persona, organización o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer clic en un enlace).
Plan de Continuidad del Negocio:	Prevé la continuidad de los servicios que el Instituto FONACOT proporciona a sus acreditados ante una contingencia, mitiga el daño económico, operacional o reputacional del Instituto FONACOT.
Política:	Son expectativas e intenciones de la organización formalmente documentadas. Las políticas se utilizan para guiar las decisiones, y para asegurar el desarrollo e implementación consistente y apropiado de procesos, normas, roles, actividades, infraestructura de TI, etc.

 TRABAJO <small>SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL</small>	MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT	Clave: MA26.01	
		Vigencia: Julio, 2024	

Concepto	Definición
Privilegios:	Permite iniciar sesión en una base de datos; crear nuevos registros, modificar registros existentes, copiar y eliminar registros.
Probabilidad:	Posibilidad de que algo suceda.
Procedimiento:	Método o modo de realizar una actividad, que consiste en secuencias cronológicas de las acciones requeridas para terminar una actividad.
Propietario de la Política:	Todo aquel servidor público, mujer u hombre laborando en el Instituto FONACOT, que realiza la gestión de la política.
Propietario del Procedimiento:	Todo aquel servidor público, mujer u hombre laborando en el Instituto FONACOT, que realiza la gestión del procedimiento.
Puerto:	Zona o localización de la memoria de un ordenador que se asocia con un puerto físico o con un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.
Puerto USB:	Es una interfaz que permite la conexión de periféricos a diversos dispositivos, entre los cuales se encuentran las computadoras, los teléfonos móviles y memorias USB.
Resguardo:	Guarda y/o custodia de algún activo del Instituto FONACOT (información, equipos de cómputo, etc.).
Responsable del MGS:	Rol encargado de vigilar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejorar del Marco de Gestión de Seguridad de la Información.
Riesgo:	Es un posible evento que podría causar daños o pérdidas, o afectar la capacidad de alcanzar objetivos. Un riesgo se mide por la probabilidad de una amenaza, la vulnerabilidad de los activos a esa amenaza, y el impacto que tendría si ocurre.
Riesgo Inherente:	Es el resultado del análisis de riesgo sin contemplar la implementación de los controles.
Riesgo Residual:	Es el resultado del análisis de riesgo contemplando la implementación de los controles.
Systems, Applications, Products in Data Processing:	Sistema informático que le permite a las organizaciones administrar sus recursos humanos, financieros, contables, productivos, logísticos y más.
Seguridad de la Información:	Preservación de la confidencialidad, integridad y disponibilidad.
Servicios Administrados:	Son servicios subcontratados con un proveedor con el objetivo de operar, mantener y dar soporte después de la adquisición de las soluciones tecnológicas, infraestructura, desarrollo o aplicativos, donde se realiza toda la configuración y manejo de las herramientas.
Servicios Informáticos:	SharePoint, Intranet, File Server, IP Communicator, entre otros.
Sistema de crédito:	Servicio integral de originación de crédito capaz de evaluar la solvencia del trabajador, su experiencia de pago, y su capacidad de pago estimada a través de su ingreso disponible, que a su vez optimiza el proceso crediticio del Instituto FONACOT mediante el uso de herramientas tecnológicas que permite automatizar, simplificar y optimizar los procesos y subprocesos para la autorización del crédito, toma de biométricos, prospección, evaluación, y contratación, utilizando tecnología de punta que proporcione máxima seguridad, confiabilidad y transparencia.

Concepto	Definición
Sistemas Operativos:	Un sistema operativo es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.
Software:	Conjunto de componentes o instrucciones lógicas que puede ejecutar una computadora.
Software como Servicio:	Servicio en la nube en la cual el proveedor proporciona al cliente un entorno de Software, así como la administración total del aplicativo.
Structured Query Language:	Lenguaje de consulta estructurada.
Transport Security Layer:	Protocolos criptográficos que proporcionan seguridad en las comunicaciones a través de Internet.
Uniform Resource Identifier:	Es una cadena de caracteres que se utiliza para identificar un nombre o un recurso web.
Uniform Resource Locator:	Se utiliza a menudo como referencia a un recurso.
Unidad Administrativa	Área que integra la estructura orgánica del Instituto FONACOT (Dirección General, Coordinaciones Generales, Subdirecciones Generales, Unidad para la Administración Integral de Riesgos, Abogado General, Dirección de Comunicación Institucional, Direcciones Comerciales Regionales, Direcciones Estatales o de Plaza, Dirección de Auditoría Interna, Direcciones de Área, Subdirecciones y Jefaturas de Departamento, contenidas en los Manuales de Organización General y Específicos del Instituto FONACOT).
Universal Serial Bus:	Periférico que permite conectar diferentes periféricos a una computadora.
Vulnerabilidad:	Es una debilidad que podría ser aprovechada por una amenaza, también se considera como vulnerabilidad la falta de un control.
Virtual Private Network:	Red Privada Virtual, la cual funciona como herramienta sencilla que protege tu privacidad en Internet y mantiene tu ubicación y tráfico ocultos.

2 ACRÓNIMOS.

Para efectos del presente Marco, se entenderá por:

Acrónimo:	Concepto:
AES:	Advanced Encryption Standard.
APT:	Advanced Persistent Threat.
ASI:	Administración de la Seguridad de la Información.
ARCO:	Acceso, Rectificación, Cancelación y Oposición.
AST:	Application Security Testing.
Buffer Overflow:	Desbordamiento de búfer.
CEDN:	Coordinación de Estrategia Digital Nacional.
CERT-MX:	Centro Especializado en Respuesta Tecnológica de la Dirección Científica de la Guardia Nacional.
BCP:	Business Continuity Plan.
CD:	Compact Disc.
CNBV:	Comisión Nacional Bancaria y de Valores.
CSF:	Cybersecurity Framework.
CREDERE:	Sistema de Crédito Institucional.
CUOEF:	Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento.
DAST:	Dynamic Application Security Testing.
DBF:	Database Firewall.
DBMS:	Database Management System.
DDoS:	Distributed Denial of Service.
DEPyR:	Direcciones Estatales, de Plaza o Representaciones.
DES:	Data Encryption Standard.
DHCP:	Dynamic Host Configuration Protocol.
DKIM:	DomainKeys Identified Mail.
DIT:	Dirección de Infraestructura Tecnológica.
DMARC:	Domain-based Message Authentication, Reporting & Conformance.
DMZ:	Demilitarized Zone.
DOF:	Diario Oficial de la Federación.
DRH:	Dirección de Recursos Humanos.
DRMySG:	Dirección de Recursos Materiales y Servicios Generales.
DRP:	Disaster Recovery Plan.
DPI:	Derechos de propiedad intelectual.
DTI:	Dirección de Tecnologías de la Información.
DVD:	Digital Versatile Disc.

Acrónimo:	Concepto:
EAP-FAST:	Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling.
EAP-TTLS:	Extensible Authentication Protocol- Tunneled Transport Layer Security.
ERISC:	Equipo de Respuesta a Incidentes de Seguridad en TIC.
FTP:	File Transfer Protocol.
HSM:	Hardware Security Module.
HTTPS:	Hypertext Transfer Protocol Secure.
IaaS:	Infrastructure as a Service.
INAI:	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto FONACOT:	Instituto del Fondo Nacional para el Consumo de los Trabajadores.
IP:	Internet Protocol.
IPC:	Inter Process Communication.
IPSEC:	Internet Protocol Security.
IPv6:	Internet Protocol versión 6.
KPI:	Key Performance Indicator.
L2TP:	Layer 2 Tunneling Protocol.
LAN:	Local Area Network.
LGPDPPO:	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
MAC Address:	Media Access Control Address.
MASVS:	Mobile Application Security Verification Standard.
MGSI:	Marco de Gestión de Seguridad de la Información.
MGT:	Management.
MSTG:	Mobile Security Testing Guide.
NIST:	National Institute of Standards and Technology.
NSTL:	National Software Testing Lab.
OICE:	Órgano Interno de Control Específico en el Instituto FONACOT.
OLA:	Operation Level Agreement.
OMS:	Organización Mundial de la Salud.
OTAN:	Organización del Tratado del Atlántico Norte.
OWASP:	Open Web Application Security Project.
PaaS:	Platform as a Service.
PAM:	Privileged Access Management.
PCN:	Plan de Continuidad de Negocio.
PEAP:	Protected Extensible Authentication Protocol.
PHVA:	Planear, Hacer, Verificar y Actuar.
PIE:	Position Independent Executables.

Acrónimo:	Concepto:
PKI:	Public Key Infraestructure.
PSK:	Phase-shift Keying.
ROM:	Read Only Memory.
RSA:	Rivest–Shamir–Adleman
RSI:	Responsable de la Seguridad de la Información en el Instituto FONACOT.
SaaS:	Software as a Service.
SAMM:	Software Assurance Maturity Model.
SANS:	SysAdmin Audit, Networking and Security Institute.
SAP:	Systems, Applications, Products in Data Processing.
SAS:	Herramienta para generación de reportes (Business Intelligence).
SAST:	Static Application Security Testing.
SAT:	Subdirección de Administración del Talento Humano.
SDLC:	Software Development Life Cycle.
SDSI:	Subdirección de Desarrollo de Sistemas e Información.
SGA	Subdirección General de Administración.
SGTIC:	Subdirección General de Tecnologías de la Información y Comunicación.
SGCyR:	Subdirección General de Crédito y Recuperación.
SIC:	Sociedades de Información Crediticia.
SIT:	Subdirección de Infraestructura Tecnológica.
SLA:	Service Level Agreement.
SPF:	Sender Policy Framework.
SQL:	Structured Query Language.
SSH:	Secure Shell.
SSID:	Service Set Identifier.
SSL:	Secure Sockets Layer.
SSOS:	Subdirección de Soporte y Operación de Sistemas.
SUDO:	Es un comando de Linux que se utiliza para la ejecución de comandos con altos privilegios (root).
TIC:	Tecnologías de la información y las comunicaciones.
TKIP:	Temporal Key Integrity Protocol.
TLS:	Transport Layer Security.
UPS:	Uninterruptible Power Supply.
URI:	Uniform Resource Identifier.
URL:	Uniform Resource Locator.
USB:	Bus universal en serie.
VNC:	Virtual Network Computing.

Acrónimo:	Concepto:
Vo. Bo.:	Visto Bueno.
VPN:	Virtual Private Network.
WAF:	Web Application Firewall.
WPA:	Wi-Fi Protected Access.
XSS:	Cross-site scripting.

TRANSITORIOS.

Primero. - Queda sin efecto el Marco de Gestión de Seguridad de la Información del Instituto FONACOT, versión MA26.00 con vigencia del 01 de noviembre de 2022.

Segundo. - El presente Manual entra en vigor a partir de su publicación en la normateca interna del Instituto FONACOT.

TERMINA MGSÍ.