Firmado digitalmente por ESQUIVEL TORRES Luis Alberto FAU 20509139700 hard
Motivo: Soy el autor del documento
Fecha: 03.06.2025 11:03:15 -05:00

RESOLUCIÓN DE DIRECCIÓN EJECUTIVA

San Isidro, 03 de Junio del 2025

RDE N° 000094-2025-MIDIS/FONCODES/DE

VISTO:

El Memorando N° 000079-2025-MIDIS/FONCODES/UTI y el Memorando N° 000151-2025-MIDIS/FONCODES/UTI de la Unidad de Tecnologías de la Información; el Memorando N° 000636-2025-MIDIS/FONCODES/UPPM y el Informe N° 000034-2025-MIDIS/FONCODES/UPPM-CROM de la Unidad de Planeamiento, Presupuesto y Modernización, el Informe N° 000191-2025-MIDIS/FONCODES/UAJ de la Unidad de Asesoría Jurídica y;

CONSIDERANDO:

Que, mediante la Ley N° 29792 se crea el Ministerio de Desarrollo e Inclusión Social, determinándose su ámbito, competencias, funciones y estructura orgánica básica; señalando en su Tercera Disposición Complementaria Final, la adscripción a dicho Ministerio, entre otros programas, al Fondo de Cooperación para el Desarrollo Social (en lo sucesivo FONCODES);

Que, el Manual de Operaciones del FONCODES, aprobado con Resolución Ministerial N° 228-2017-MIDIS, establece en el artículo 9, literal i), como función de la Dirección Ejecutiva, la de emitir Resoluciones de Dirección Ejecutiva en asuntos de su competencia;

Que, el citado Manual de Operaciones, establece en el literal b) de su artículo 21 como una de las funciones de la Unidad de Tecnologías de la Información la de formular políticas, normas, metodologías y estándares para la administración, implementación y uso eficiente de las tecnologías de información, así como de la seguridad de la infraestructura tecnológica y de soluciones informáticas;

Que, a través de la Resolución Ministerial N° 002-2021-MIDIS se aprueban los “Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social”, la misma que señala en su artículo 3 que los Programas Nacionales adscritos al citado Ministerio, en lo que corresponda, deben adecuar sus protocolos o lineamientos internos, a las disposiciones previstas en los Lineamientos aprobados;

Que, a través de la Resolución de Dirección Ejecutiva N° 000135-2021-FONCODES/DE se aprueba la versión 1.0 de la Directiva N° 31-2021-FONCODES/UTI “Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES”;

Que, la Directiva N° 003-2022-MIDIS: Catálogo de Documentos Oficiales del Ministerio de Desarrollo e Inclusión Social – MIDIS: aprobada por Resolución Ministerial N° 159-2022-MIDIS, señala en el ítem 4.2.2 del subnumeral 4.2 del numeral 4, que la Directiva es el documento normativo que regula aspectos vinculados al funcionamiento del Ministerio de Desarrollo e Inclusión Social en el marco de sus funciones como rector del Sistema Nacional de Desarrollo e Inclusión Social o en el caso de los Programas Nacionales, para regular aspectos enmarcados en las funciones establecidas en su Manual de Operaciones. También se utiliza cuando se requiera regular la implementación de los sistemas administrativos desde el Ministerio de Desarrollo e Inclusión Social con alcance o aplicación en los Programas Nacionales, indicando, además, que la Directiva es aprobada por el Titular del Programa Nacional;

Que, asimismo, la Directiva precitada establece en el ítem 5.4.1.4 del párrafo 5.4.1 del subnumeral 5.4 del numeral 5, que los documentos normativos se actualizan para fines de mejora de los procesos involucrados, y/o por modificaciones en la normativa aplicable al documento, y/o por cambios organizativos, y/o por otros mandatos en normas nacionales, precisando que en la actualización, los cambios en el documento normativo son estructurales, por tanto, se realiza la derogación del mismo y se procede a actualizar, iniciando una nueva versión del documento normativo;

V°B° Digital
Firmado digitalmente por GARCIA MONTANEZ Santiago Ivan FAU 20509139700 hard
Motivo: Doy V° B°
Fecha: 03.06.2025 10:27:18 -05:00

V°B° Digital
Firmado digitalmente por QUISPE CHAVEZ Ynes Aurora FAU 20509139700 hard
Motivo: Doy V° B°
Fecha: 03.06.2025 09:27:13 -05:00

V°B° Digital
Firmado digitalmente por ROJAS ALVAREZ Ronny FAU 20509139700 hard
Motivo: Doy V° B°
Fecha: 03.06.2025 08:34:20 -05:00

Que, mediante Resolución de Dirección Ejecutiva N° 150-2018-FONCODES/DE, se aprueba el Procedimiento N° 86-2018-FONCODES/UPPM-CROM "Control de Documentos Normativos", que tiene como objetivo, establecer las disposiciones para la elaboración, actualización y control de los documentos normativos en sus etapas de acciones previas, elaboración, revisión, aprobación, distribución, registro e implementación; precisando en el ítem 4.2.3 del subnumeral 4.2 del numeral 4, que la Directiva es el documento que establece y desarrolla las disposiciones para la implementación de las políticas o lineamientos institucionales en base a lo señalado por el sector, o que determina procedimientos y acciones técnicas o administrativas, respecto a una materia específica, en cumplimiento de las disposiciones legales vigentes; asimismo, el numeral 7.6 de dicha norma, prescribe que los documentos normativos son aprobados por el Director Ejecutivo mediante Resolución de Dirección Ejecutiva;

Que, asimismo, la disposición precitada establece en el numeral 4.7, que los cambios mayores son las modificaciones a los documentos normativos vigentes que conllevan la necesidad de cambios significativos en el contenido del documento normativo o como consecuencia de modificaciones recurrentes y/o consecutivas, siendo que, en esos casos, se cambiará la versión del documento, añadiéndose en el numeral 7.8, que, en el caso de cambios mayores corresponde aprobar una nueva versión del documento normativo, dejando sin efecto la versión anterior;

Que, mediante el Memorando N° 000079-2025-MIDIS/FONCODES/UTI y el Memorando N° 000151-2025-MIDIS/FONCODES/UTI, la Unidad de Tecnologías de la Información sustenta la necesidad de actualizar la versión 1.0 de la Directiva N° 31-2021-FONCODES/UTI "Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES"; y precisa que la misma responde a observaciones de auditoría y a los cambios derivados de la actualización de la norma NTP-ISO/IEC 27001:2014 a la versión NTP-ISO/IEC 27001:2022, bajo la denominación "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información - Requisitos", por lo que remite el citado documento para el trámite de aprobación por la Dirección Ejecutiva;

Que, mediante el Memorando N° 000636-2025-MIDIS/FONCODES/UPPM y el Informe N° 000034-2025-MIDIS/FONCODES/UPPM-CROM la Unidad de Planeamiento, Presupuesto y Modernización, emite conformidad al proyecto de la versión 2.0 de la Directiva N° 31-2025-FONCODES/UTI "Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES, en el marco de lo establecido en la Directiva N° 003-2022-MIDIS "Catálogo de Documentos Oficiales del Ministerio de Desarrollo e Inclusión Social-MIDIS" y el Procedimiento N° 86-2018-FONCODES/UPPM-CROM "Control de Documentos Normativos"; precisando que el citado documento normativo, cumple con los criterios de consistencia y coherencia que todo documento normativo del FONCODES debe cumplir; y recomienda proseguir su trámite;

Que, a través del Informe N° 000191-2025-MIDIS/FONCODES/UAJ, la Unidad de Asesoría Jurídica de acuerdo con la evaluación y análisis de la documentación remitida, considera procedente, en los aspectos legales y formales la emisión de la Resolución de Dirección Ejecutiva que aprueba la versión 2.0 de la Directiva N° 31-2025-FONCODES/UTI "Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES", cuyo objetivo es establecer los lineamientos y acciones para mejorar la seguridad de la información y confianza digital en la entidad, dejando sin efecto, asimismo, la versión 1.0 de la Directiva N° 31-2021-FONCODES/UTI;

Que, estando a los considerandos precedentes resulta necesario emitir el acto administrativo que aprueba la versión 2.0 de la Directiva N° 31-2025-FONCODES/UTI "Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES",

Con las visaciones de la Unidad de Tecnologías de la Información, la Unidad de Planeamiento, Presupuesto y Modernización y la Unidad de Asesoría Jurídica;

De conformidad con la Ley N° 29792, Ley de creación, organización y funciones del MIDIS, y de acuerdo a las facultades otorgadas en el Manual de Operaciones de FONCODES, aprobado mediante Resolución Ministerial N° 228-2017-MIDIS.

SE RESUELVE:

Artículo 1.- Aprobación de Directiva

Aprobar la versión 2.0 de la Directiva N° 31-2025-FONCODES/UTI “Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES”, que forma parte integrante de la presente Resolución.

Artículo 2.- Dejar sin efecto

Dejar sin efecto la versión 1.0 de la Directiva N° 31-2021-FONCODES/UTI “Disposiciones para la Gestión de la Seguridad de la Información en el FONCODES”, aprobada mediante Resolución de Dirección Ejecutiva N° 000135-2021-FONCODES/DE, de acuerdo a los argumentos expuestos en la parte considerativa de la presente Resolución.

Artículo 3.- Disposición

Disponer que la Unidad de Tecnologías de la Información, las Unidades Orgánicas y Unidades Territoriales competentes adopten las acciones necesarias para el debido cumplimiento de la Directiva que hace referencia el artículo 1 de la presente Resolución.

Artículo 4.- Publicación

Disponer la publicación de la presente Resolución en el portal institucional del FONCODES (http://www.gob.pe/foncodes).

REGÍSTRESE Y COMUNÍQUESE.

Documento firmado digitalmente

……..

LUIS ALBERTO ESQUIVEL TORRES
Director Ejecutivo del FONCODES
FONDO DE COOPERACIÓN PARA EL DESARROLLO SOCIAL

DISPOSICIONES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL FONCODES

Directiva N° 31 - 2025-FONCODES/UTI

Versión N° 2.0

Aprobado mediante Resolución de Dirección Ejecutiva N° 094-2025-FONCODES/DE

Etapa	Responsable	Cargo	Visto Bueno y sello:
Formulado por:	Juan Carlos Reátegui Morales	Oficial de Seguridad de la Información y Confianza Digital	FONCODES Firma Digital — Firmado digitalmente por REATEGUI MORALES Juan Carlos FAU 20509139700 soft. Motivo: Soy el autor del documento. Fecha: 13.05.2025 15:53:51 -05:00
Revisado por:	Santiago Iván Garcia Montañez	Jefe de la Unidad de Tecnologías de la Información	FONCODES Firma Digital — Firmado digitalmente por GARCIA MONTAÑEZ Santiago Ivan FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 13.05.2025 16:34:13 -05:00
	Edgard Alberto Juarez Baldera	Jefe de la Unidad de Administración	FONCODES Firma Digital — Firmado digitalmente por JUAREZ BALDERA Edgard Alberto FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 13.05.2025 19:09:34 -05:00
	Mariella Sussy Sarmiento Caballero	Jefe de la Unidad de Recursos Humanos	FONCODES Firma Digital — Firmado digitalmente por SARMIENTO CABALLERO Mariella Sussy FAU 20509139700 soft. Motivo: Soy el autor del documento. Fecha: 14.05.2025 10:46:09 -05:00
	Ynes Aurora Quispe Chavez	Jefa de la Unidad de Planeamiento, Presupuesto y Modernización	FONCODES Firma Digital — Firmado digitalmente por QUISPE CHAVEZ Ynes Aurora FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 15.05.2025 14:37:32 -05:00
	Ronny Rojas Álvarez	Jefe de la Unidad de Asesoría Jurídica	FONCODES Firma Digital — Firmado digitalmente por ROJAS ALVAREZ Ronny FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 30.05.2025 15:55:04 -05:00
	Santos Enrique Quedena Zambrano	Coordinador (e) de Racionalización, Organización y Métodos	FONCODES Firma Digital — Firmado digitalmente por QUEDENA ZAMBRANO Santos Enrique FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 14.05.2025 14:46:09 -05:00
Aprobado por:	Luis Alberto Esquivel Torres	Director Ejecutivo	FONCODES Firma Digital — Firmado digitalmente por ESQUIVEL TORRES Luis Alberto FAU 20509139700 hard. Motivo: Soy el autor del documento. Fecha: 03.06.2025 08:15:13 -05:00

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Documento sustento	Textos modificados	Responsable
1.0	26.11.21	Memorando Múltiple N° 0005-2021-MIDIS-FONCODES/UTI	Versión inicial	Unidad de Tecnologías de la Información
2.0	01.03.25	Memorando N° 0079-2025-MIDIS-FONCODES/UTI	Diversos componentes de la versión 1.0 de la Directiva.	Unidad de Tecnologías de la Información

Notas:
1/ Señalar el informe que sustenta la formulación del documento normativo y/o el informe que sustenta la modificación de la nueva versión del documento.
2/ Señalar los artículos, numerales, literales, anexos, etc. que genera la modificación del documento.
3/ Señalar la unidad de organización que formula la nueva versión del documento.

1. **OBJETIVO**

   Establecer los lineamientos y acciones para mejorar la seguridad de la información y confianza digital en el Fondo de Cooperación para el Desarrollo Social – FONCODES.

2. **ÁMBITO DE APLICACIÓN**

   La presente directiva es de cumplimiento obligatorio por todos los servidores civiles de las unidades de organización del FONCODES.

3. **BASE LEGAL**

   3.1. Ley N°27806, Ley de Transparencia y Acceso a la Información Pública y sus modificatorias.

   3.2. Ley N°30096, Ley de Delitos Informáticos y sus modificatorias.

   3.3. Ley 29733, Ley de Protección de Datos Personales y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS.

   3.4. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y sus modificatorias.

   3.5. Decreto Supremo N°024-2006-PCM, que aprueba el Reglamento de la Ley Nº 28612, Ley que norma el uso, adquisición y adecuación de software en la administración pública.

   3.6. Decreto Supremo N°003-2013-JUS, que aprueba el reglamento de la Ley N°29733, Ley de Protección de Datos Personales y modificatorias.

   3.7. Decreto Supremo N° 016-2017-PCM, que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales 2017 - 2021 y del Modelo de Datos Abiertos Gubernamentales del Perú.

   3.8. Decreto Supremo N° 050-2018-PCM, que aprueba la definición de Seguridad Digital en el Ámbito Nacional.

   3.9. Decreto Supremo N° 029-2021-PCM , que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

   3.10. Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública.

   3.11. Resolución de Contraloría N° 320-2006-CG, que aprueba Normas de Control Interno.

   3.12. Resolución Ministerial N° 04-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP –ISO/IEC 27001:2014 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática y modificatoria.

   3.13. Resolución de la Dirección Ejecutiva N° 021-2016-FONCODES-DE, que aprueba el Reglamento Interno de los Servidores-RIS.

   3.14. Decreto Supremo N° 016-2017-PCM, que aprueba la Estrategia Nacional de Datos Abiertos Gubernamentales 2017 - 2021 y del Modelo de Datos Abiertos Gubernamentales del Perú.

   3.15. Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.

   3.16. Resolución Ministerial N° 169-2019-MIDIS, que modifica la Resolución Ministerial N° 192-2018-MIDIS, Constituir el Comité de Gobierno Digital en el Ministerio de Desarrollo e Inclusión Social.

   3.17. Resolución Ministerial N° 002-2021-MIDIS, que aprueba los Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e inclusión Social.

   3.18. Resolución Ministerial N° 320-2021-PCM, aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".

3.19. Resolución de Secretaría de Gobierno Digital N° 003-2018-PCM/SEGDI, que aprueba la Guía para la formulación del Plan de Gobierno Digital y establecen disposiciones adicionales para la planificación del Gobierno Digital.

3.20. Resolución de Dirección Ejecutiva N° 131-2017-FONCODES-DE, que designa al Oficial de Seguridad de Información.

3.21. Resolución de Dirección Ejecutiva N° 104-2023-FONCODES-DE CSIRT Conformación del Equipo de Respuesta ante Incidentes de Seguridad.

3.22. Resolución de Dirección Ejecutiva N° 182-2023-FONCODES/DE, que aprueba la conformación del Grupo Comando de la Gestión de Continuidad Operativa del FONCODES.

3.23. Resolución de Dirección Ejecutiva N° 104-2023-FONCODES/DE, conformación del Equipo de Respuesta ante Incidentes de Seguridad Digital del FONCODES.

3.24. Norma Técnica Peruana ISO 22301:2013 Protección y Seguridad de los Ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones.

3.25. Norma Técnica Peruana NTO-ISO/IEC 27001:2022. Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.

3.26. Resolución de Dirección Ejecutiva N° 000173-2024-FONCODES/DE, aprobar la versión N° 1 del Plan N° 073-2024-MIDIS-FONCODES/UTI "Plan de Recuperación de los Servicios de la Tecnología de la Información".

4. DEFINICIONES

4.1. **Acceso privilegiado:** Es el acceso a información crítica o confidencial que se otorga de manera temporal a personas debidamente autorizadas.

4.2. **Activo Informático**: Conjunto de bienes de una organización que se encuentran relacionados directa o indirectamente con la actividad informática. Entre ellos se encuentran:

a). Equipo informático
b). Licencias de Software
c). Los aplicativos informáticos y/o software de la institución, ya sea desarrollados por ésta, adquiridos o alquilados a terceros.
d). La información institucional.
e). Las redes de datos, comunicaciones y los equipos que se deriven para conformación de la Red Informática.
f). Los medios magnéticos y ópticos de almacenamiento de la información (cintas, cartuchos, CD, DVD, BluRay, Memorias USB, entre otros.).
g). Los manuales, procedimientos y reglamentaciones afines con actividad informática.

4.3. **Activo de Información**: Es el elemento de información que FONCODES recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

4.4. **Amenaza(s):** Causa potencial de un incidente no deseado que puede resultar en daño a los activos informáticos, servicios informáticos, sistemas u organización.

Es un evento o incidente provocado por una entidad hostil a FONCODES (humana, natural o artificial), que aprovecha una o varias vulnerabilidades de un activo con el fin de agredir la confidencialidad, integridad o disponibilidad de ese mismo activo o de otros activos de la organización (se dice que la amenaza explota la vulnerabilidad del activo).

Las amenazas pueden ser externas o internas a la organización y pueden ser deliberados o accidentales (por ejemplo, un desastre natural o negligencia sin intención de daño por parte de servidor civil de la organización).

Otro ejemplo: Errores - Daño intencional/Ataque, Robo, Falla de equipo/software, Desastre natural.

4.5. **Aplicativos Informáticos:** Software desarrollado por la institución o adquiridos a terceros para la ejecución de sus actividades u operaciones (Sistema de Trámite Documentario, Sistema de Gestión de Proyectos, Sistema de Gestión Administrativa, entre otros).

4.6. **Confianza Digital:** Estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales. Su propósito es impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital. Tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

4.7. **Colaboradores:** Personas que no tienen vínculo laboral con la institucón, sin embargo, hacen uso de un activo y/o servicio informático en forma temporal y debidamente autorizado.

4.8. **Datos sensibles.** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

4.9. **Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT):** es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a la RDE N° 104-2023-FONCODES/DE.

4.10. **Equipo Informático:** Computadoras, Laptops, Notebooks, Impresoras, Escáneres, equipo-Servidor, entre otros bienes tangibles afines.

4.11. **Equipo-Servidor:** Es un ordenador u otro tipo de dispositivo que suministra una información requerida por unos clientes (que pueden ser personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras, etc.).

4.12. **Evaluación de Riesgos:** Es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, las probabilidades que ocurran los hechos y su potencial impacto en las operaciones del FONCODES.

4.13. **Gobierno Digital:** es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

4.14. **Incidente de seguridad de información:** Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

4.15. **Instalaciones de proceso de información:** Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

4.16. **Propietario de la Información:** El término "propietario" identifica a un individuo de la entidad que tiene la responsabilidad de la gestión de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. El término "propietario" no significa que la persona tiene algún derecho de propiedad realmente sobre el activo de información.

4.17. **Responsable de Informática:** Es el responsable de Tecnología de Información (TI), en el caso del FONCODES se denomina actualmente Jefe(a) de Unidad de Tecnologías de la Información.

4.18. **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias. El riesgo se puede definir, desde varios puntos de vista y enfoques, es conceptualizado como "la

probabilidad de que un evento adverso ocurra durante un periodo determinado de tiempo, o resulte de una situación particular. Es la probabilidad de que ocurra o se presente un fenómeno natural o antropogénico destructivo en el ámbito de un sistema afectable. Es considerado también como el resultado de un proceso mental. El estímulo es el "peligro", o sea el objeto o actividad con el potencial de ocasionar un perjuicio o causar un daño. Existen actualmente diversos enfoques sobre el concepto de riesgo, el cual puede estudiarse desde el punto de vista ambiental, social, cultural, salud pública, económica y política.

4.19. **SLA:** Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio, por lo tanto:

a). El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, servidor civil asignado al servicio, etc. Básicamente el ANS define la relación entre ambas partes: proveedor y cliente. Un ANS identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

b). El ANS se caracteriza por ser un proceso estructurado, una metodología homogénea que promueve la convergencia organizacional. Suele incluir herramientas para hacer benchmarking internos, y proporciona una visión multidimensional de las interrelaciones entre los distintos servicios.

c). También constituye un punto de referencia para el mejoramiento continuo, ya que el poder medir adecuadamente los niveles de servicio es el primer paso para mejorarlos y de esa forma aumentar los índices de calidad.

4.20. **Seguridad de la información:** Las medidas correctivas y proactivas para la preservación de la confidencialidad, integridad y disponibilidad de la información.

4.21. **Seguridad Digital:** es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

4.22. **Servicio Informático:** Conjunto de actividades o tareas asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios de este recurso.

4.23. **Trabajo Remoto:** la prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita. Este se extiende a cualquier tipo de trabajo que no requiera la presencia física del trabajador en el centro de labores.

4.24. **Usuario:** Los/las servidores/as de FONCODES u otra persona que haga uso de un recurso informático o servicio de la tecnología de la información para fines laborales.

4.25. **Vulnerabilidad:** Debilidad de un activo o grupo de activos informáticos que pueden ser alterados en su normal funcionamiento por una o más amenazas, según lo siguiente:

a). Condiciones determinadas por factores o procesos físicos, sociales, económicos, y ambientales, que aumentan la susceptibilidad de la institución al impacto de amenazas.

b). Una vulnerabilidad es toda aquella circunstancia o característica de un activo que permite la consecución de ataques que comprometen la confidencialidad, integridad o disponibilidad de ese mismo activo o de otros activos de la organización.

c). La vulnerabilidad ante un desastre dado es la capacidad de respuesta ante el fenómeno, es decir, que un objeto sea vulnerable a un fenómeno determinado es, en primera instancia, que sea susceptible de sufrir daños por la acción de este fenómeno; ahora bien, si se entiende como objeto cualquier objetivo social o económico, entonces la vulnerabilidad estará en dependencia de las características específicas del fenómeno, así como del objeto cuya vulnerabilidad se desee evaluar. La vulnerabilidad no es estática, sino un proceso dinámico en dependencia de las condiciones tanto naturales como sociales.
Ejemplo: Falta de conocimiento del usuario, falta de funcionalidad de la seguridad, configuración inadecuada del cortafuego, elección deficiente de contraseñas, tecnología no probada, transmisión por comunicaciones no protegidas, inexistencia de sistema contra incendio.

5. RESPONSABILIDADES

5.1. los Jefes de Unidad, Coordinadores, Jefes de Unidades Territoriales de FONCODES y los usuarios de los sistemas informáticos son responsables de la aplicación de la presente directiva, por lo que deben velar por su cumplimiento, de acuerdo a sus competencias.

5.2. Los jefes de Unidad, Coordinadores, Jefaturas de Unidades Territoriales y usuarios, son responsables de la información y documentación que generen y administren directamente en cumplimiento de sus funciones y competencias, así como de los activos y servicios informáticos que utilicen o autoricen su asignación o uso.

5.3. Los jefes de Unidad, Coordinadores, Jefaturas de Unidades Territoriales y usuarios, son responsables de velar por la seguridad de su información, evaluar los riesgos e informar sobre el mal uso que se le pueda estar dando a un activo o servicio informático.

6. DISPOSICIONES GENERALES

6.1. La Unidad de Tecnologías de la Información, en adelante UTI, es la unidad encargada del desarrollo y administración de los sistemas y servicios informáticos del FONCODES, así como de la evaluación técnica para la adquisición de los activos y servicios informáticos a terceros.

6.2. La UTI, es la encargada de velar por la protección de la información institucional que administra; para lo cual dispone de los mecanismos de almacenamiento, seguridad y protocolos de contingencias ante cualquier riesgo.

6.3. La UTI de acuerdo a su competencia podrá restringir el uso de servicios informáticos, dispositivos informáticos, equipos informáticos u otros debido al uso incorrecto de estos, o en el caso de presentar un peligro para la seguridad de información.

7. DISPOSICIONES ESPECÍFICAS DE SEGURIDAD DE INFORMACIÓN

7.1 Controles organizacionales

7.1.1 Políticas para la seguridad de la información

El objetivo es proporcionar dirección y apoyo de la alta dirección para la seguridad de información en concordancia con los requisitos del negocio y las leyes regulares relevantes.

La Política de Seguridad de Información, es la establecida por el Sector MIDIS y está dada por la RM N° 002-2021-MIDIS, aprobar los "Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social.

FONCODES coordinará las actualizaciones con el Sector MIDIS, si hubiere algunos cambios que lo ameriten.

7.1.2 Roles y responsabilidades en seguridad de la información

El objetivo es establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de FONCODES.

El FONCODES ha definido los roles y responsabilidades para la seguridad de información en:

a) Comité de Gobierno y Transformación Digital

Gestionar la asignación del servidor civil y recursos necesarios para la implementación del SGSI en los Planes Operativos Institucionales, Cuadro Multianual de Necesidades, Plan Anual de Contrataciones, según corresponda, entre otros.

- Elaborar informes anuales que evalúen el desempeño del SGSI.
- Gestionar, mantener y documentar el SGSI de la entidad.

b) Unidad de Tecnologías de la Información

- Establecer, mantener y documentar el sistema de seguridad de la información en el marco de la normativa vigente.
- Administrar los procesos de seguridad de la información.
- Proponer las directrices necesarias para la implementación de las soluciones tecnológicas en la entidad.
- Identificar, gestionar y actualizar los riesgos e incidentes de seguridad de la información en FONCODES, asegurando su tratamiento oportuno, en coordinación con la o el Oficial de Seguridad de la Información.

c) Oficial de Seguridad de la Información

- Asegurar que el SGSI esté conforme a los requisitos de la NTP ISO/IEC 27001:2022.
- Reportar el desempeño del SGSI al Comité de Gobierno y Transformación Digital
- Mantener actualizado los documentos generados en el marco del SGSI.
- Asistir al servidor civil de la entidad y a las personas que presten servicios cualquiera sea su condición o modalidad contractual en materia de seguridad de la información.
- Coordinar con la Secretaría de Gobierno y Transformación Digital de la PCM el cumplimiento de las disposiciones en materia de seguridad de la información.
- Analizar en coordinación con los responsables de los órganos, el riesgo de los accesos de terceros a la información de la entidad y verificar la aplicación de las medidas de seguridad necesarias para la protección de la misma, en coordinación con la Unidad de Tecnologías de la Información.
- Revisar los riesgos de seguridad de la información de la entidad y coordinar la elaboración de los planes de tratamiento, en coordinación con las y los responsables de los órganos y la Unidad de Planeamiento, Presupuesto y Modernización en su calidad de órgano técnico en la implementación de la gestión de riesgos.
- Identificar las actividades de difusión y sensibilización en seguridad de la información.

- Evaluar y canalizar, de corresponder, los reportes por incumplimiento de los requisitos del SGSI, al Comité de Gobierno y Transformación Digital de FONCODES, para que evalúe las acciones pertinentes.

d) Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT)

- Coordinar con el Oficial de Seguridad de Información en lo relacionado con la implementación, mantenimiento o mejora del SGSI en la entidad.
- En coordinación con el Oficial de Seguridad de la Información, realizar el seguimiento al cumplimiento de los requisitos de la NTP ISO/IEC 27001:2022 en la entidad, así como los demás requisitos aplicables en materia de seguridad de la información.
- Afrontar proactivamente los procesos de ciberseguridad que se requieran en FONCODES.

7.1.3 Segregación de funciones

Funciones en conflicto y áreas de responsabilidad en conflicto deben ser segregadas.

Los deberes y áreas de responsabilidad deben estar segregados para reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la institución.

La segregación de funciones se refleja en el MOP de la entidad.

7.1.4 Responsabilidades de la alta dirección

La alta dirección debe requerir a todo servidor civil de FONCODES, incluyendo proveedores y personal eventual, que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas, normativas y procedimientos específicos de la organización.

7.1.5 Contacto con autoridades relacionadas con la seguridad de información

La organización debe establecer y mantener contacto con las autoridades pertinentes.

FONCODES, a través del Oficial de Seguridad de la Información debe mantener contactos apropiados con las autoridades relevantes, para el caso de Seguridad de Información. Por ejemplo, bomberos, Municipalidad, SGTD-PCM, y jefes de Áreas de TI de Ministerios o Instituciones del Sector, para colaboración en caso de desastres

7.1.6 Contacto con grupos especiales de interés

La Unidad de Tecnología de la Información (UTI), deberá mantener contacto con los grupos especiales de interés, especialistas en seguridad de información, foros especializados, para coordinar la mejora continua de la seguridad de la información en FONCODES y a nivel sectorial.

7.1.7 Inteligencia de amenazas

La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia sobre las amenazas. Coordinando con Presidencia del Consejo de Ministros, Ministerio de Defensa, MIDIS y otras instituciones pertinentes.

7.1.8 Seguridad de la información en la gestión de proyectos

La seguridad de la información debe estar integrada en la gestión de proyectos.

Los servicios de Consultoría y Asesoría que tengan relación con la elaboración de proyectos, prototipos, Planes de Gobierno Digital u otros asociados a los procesos

de UTI, deben seguir los lineamientos de seguridad de la ISO 27001 y deben ser monitoreados por la UTI.

7.1.9 Inventario de información y otros activos asociados

Un inventario de información y otros activos asociados, incluidos los propietarios, debe ser desarrollado y mantenido

En el inventario de activos informáticos, se procede a identificar los activos y/o dispositivos informáticos, que están asociados a los sistemas de información, sus respectivos propietarios y su ubicación, para elaborar un inventario con dicha información.

El referido inventario debe ser actualizado, ante cualquier modificación de la información registrada y revisado con una periodicidad mínima de un año.

El inventario inicialmente debe realizarse por:

a Equipos informáticos

b Dispositivos periféricos y de comunicaciones

c Aplicativos informáticos

d Sistemas operativos

e Bases de datos

El encargado de elaborar el inventario y mantenerlo actualizado es cada responsable de la Unidad de Organización, con este fin la UTI, hará llegar un reporte inicial del inventario y los formatos para complementar éste, los cuales deben ser remitidos al jefe de la UTI, con el visto bueno del responsable de la Unidad Organizativa.

Asimismo, cada responsable de la Unidad de Organización de la Sede Central, Sede La Molina o UT, es responsable de velar por que los activos, que estén operativos, coordinando su seguridad y mantenimiento, con los entes administrativos pertinentes.

7.1.10 Uso aceptable de la información y otros activos asociados

Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe ser identificada, documentada e implementada.

El servidor civil y proveedores o contratistas de FONCODES comprendan que los activos de información tales como equipos (por ej., PCs, laptops, medios de almacenamiento, dispositivos móviles, etc.), el acceso a Internet, las aplicaciones y los servicios de mensajería electrónica son exclusivamente para fines laborales. Bajo esta premisa se considera que se hace un uso aceptable de los activos informáticos.

Como uso aceptable de activos se considera que:

- Los servidores civiles no deberán utilizar los servicios de Internet o de correo electrónico de FONCODES para ver, descargar, guardar, recibir o enviar material relativo a o incluyendo:
- Material pornográfico.
- Fomentar la discriminación basada en la etnia, sexo, nacionalidad, edad, estado civil, orientación sexual, religión o discapacidad.
- Comportamiento amenazante o violento.
- Temas políticos.
- Actividades ilegales

- Juegos de apuestas
- Reenvío de “cadenas” por correo electrónico
- Envíos masivos de correos electrónicos no solicitados desde una cuenta o de equipo de FONCODES.

7.1.11 Devolución de activos

El servidor civil y otras partes interesadas, según sea apropiado, deben devolver todos los activos de la organización en su posesión cuando cambien o terminen su empleo, contrato o acuerdo.

Todos los servidores civiles que requieren por sus labores llevar algunos activos fuera de las instalaciones de FONCODES, deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo, bajo responsabilidad.

La Coordinación de Logística, a través de Patrimonio llevará el control de entrada y salida de activos de FONCODES.

7.1.12 Clasificación de la información

La información debe ser clasificada de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas pertinentes.

El objetivo es asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la FONCODES.

Las Unidades de organización del FONCODES deben clasificar la información de la cual es propietario, para cuyo efecto tendrán que evaluar y valorar las características de seguridad, confidencialidad, integridad y disponibilidad, tal como se especifica a continuación:

a) CONFIDENCIALIDAD:

(PUBLICA)

0- Información que puede ser conocida y utilizada sin autorización, por cualquier persona, sea servidor o no de FONCODES.

(RESERVADA – USO INTERNO)

1- Información que puede ser conocida y utilizada por todos los servidores civiles de FONCODES y algunas entidades externas, debidamente autorizadas y cuya divulgación o uso no autorizados, podría ocasionar riesgos o pérdidas leves para el FONCODES, el Sector Público Nacional o terceros.

(RESERVADA – CONFIDENCIAL)

2- Información que sólo puede ser conocida y utilizada por un grupo de usuarios que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados, podría ocasionar pérdidas significativas a FONCODES, al Sector Público Nacional o a terceros.

(RESERVADA SECRETA)

3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de usuarios, generalmente de la alta dirección de FONCODES, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.

b) INTEGRIDAD:

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad de FONCODES.

1- Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para FONCODES, el Sector Público Nacional o terceros.

2- Información cuya modificación no autorizada es de difícil reparación, y podría ocasionar pérdidas significativas para FONCODES, el Sector Público Nacional o terceros.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a FONCODES, al Sector Público Nacional o a terceros.

c) DISPONIBILIDAD:

0- Información cuya inaccesibilidad permanente no afecta las operaciones de FONCODES.

1- Información cuya inaccesibilidad permanente o durante un plazo no menor a una semana podría ocasionar pérdidas significativas para FONCODES, el Sector Público Nacional o terceros.

2- Información cuya inaccesibilidad permanente o durante un plazo no menor a un día, podría ocasionar pérdidas significativas a FONCODES, al Sector Público Nacional o a terceros.

3- Información cuya inaccesibilidad permanente o durante un plazo no menor a una hora podría ocasionar pérdidas significativas a FONCODES, al Sector Público Nacional o a terceros.

d) Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías, según valores asignados:

- CRITICIDAD BAJA: Ninguno de los valores supera el 1.
- CRITICIDAD MEDIA: Alguno de los valores es 2.
- CRITICIDAD ALTA: Alguno de los valores es 3.

e) Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

f) Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

En adelante se debe mencionar como “información clasificada” (o “datos clasificados”), a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad, conforme el cuadro adjunto:

1 Asimismo, los datos sensibles, conceptualizados como los datos personales, constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e

información relacionada a la salud o a la vida sexual, son considerados como de criticidad alta e información clasificada.

7.1.13 Etiquetado de la información

Un conjunto de procedimientos apropiado para el etiquetado de información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.

Todo activo de información debe tener una marca o señal o etiqueta, para identificarlo, a efectos del cumplimiento de la ISO 27001, el control 5.13 indica que: “Un conjunto de procedimientos apropiado para el etiquetado de información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización”.

7.1.14 Transferencia de información

Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones para transferencia, dentro de la organización y entre la organización y otras partes.

El objetivo es mantener la seguridad en la información transferida dentro de la organización y con cualquier entidad externa.

Toda transferencia de información a través de la red, deberá ser autorizada por la Jefatura de UTI.

Se llegarán a acuerdos escritos para dirigir la transferencia segura de información de FONCODES con otras entidades del Sector u otros sectores del Estado Peruano.

Los mensajes electrónicos emitidos por la UTI deben ser secuenciados y protegidos como evidencias para efectos de auditoría y control administrativo y operacional.

7.1.15 Control de acceso

Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos del negocio y de seguridad de la información

El objetivo es limitar el acceso a la información y a las instalaciones de procesamiento de la información.

La cuenta de usuario, permite a una persona identificarse ante la red informática de FONCODES y acceder a los servicios y sistemas de información que la UTI pone a disposición. El mecanismo para validar la identidad del usuario es la contraseña, por lo que ésta debe ser administrada con prudencia y responsabilidad por el usuario y solamente a los servicios autorizados.

Estos accesos serán controlados por la UTI, cruzando información con las Unidades y Coordinaciones.

7.1.16 Gestión de identidades

El ciclo de vida completo de identidades debe ser gestionado.

El objetivo es asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado los sistemas y servicios.

Los accesos a la Red y los Servicios proporcionados a través de la Red, serán otorgados únicamente a solicitud de los jefes de las Unidades o Coordinaciones, y serán especificados formalmente, debiéndose dejar evidencia capaz de ser auditada.

La gestión de cuentas de usuario está definida en el Procedimiento N° 97-2019-FONCODES/UTI: “Procedimiento de Gestión de cuentas de usuario”.

7.1.17 Información de autenticación

La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, incluyendo el asesoramiento al servidor civil sobre el manejo adecuado de la información de autenticación.

La contraseña de la red es de uso personal y exclusivo del usuario asignado y no podrá darla a conocer ni ser usada, por otros usuarios o terceros.

Con la finalidad de cumplir con las prácticas básicas de seguridad, se ha establecido los siguientes parámetros para la administración de contraseñas:

a) Longitud mínima de 8 caracteres, no se permiten contraseñas en blanco.

b) Utilizar una combinación de letras mayúsculas, minúsculas, números y caracteres especiales (por lo menos la combinación de tres de estos tipos de caracteres).

c) El período de vigencia es de 90 días calendarios

d) La contraseña será reutilizable sólo después de 10 cambios.

Para la elección y protección de contraseñas se debe tener en consideración las siguientes recomendaciones:

a) No escribir nunca una contraseña en un papel que pudiera ser leído por terceros.

b) No utilizar nombres de personas, personajes, el mismo nombre de usuario, de la institución o términos comunes.

c) No utilizar fechas de cumpleaños, aniversarios, números de teléfono u otros

d) No utilizar patrones simples o repetitivos, ejemplo; “aaaa”, “123456”, “qwerty”, etc.

e) Adicionalmente, en caso de que el usuario administre otras contraseñas debe aplicar las mismas reglas aquí señaladas.

Los accesos privilegiados solo proceden con autorización de la Jefatura de UTI y se guardará un control constante de quienes lo poseen.

La gestión de información de autentificación secreta de los usuarios, será manejada por el Administrador de Red, valiéndose del software del sistema de seguridad que proporciona el sistema operativo de la red.

7.1.18 Derechos de acceso

Los derechos de acceso a la información y otros activos asociados deben ser aprovisionados, revisados, modificados y removidos en concordancia con la política específica de la organización y las reglas para el control de acceso

Los derechos de acceso y las remociones de acceso a los usuarios se revisan periódicamente, y solo son actualizados por pedido de los jefes de Unidad o Coordinadores, de lo cual se guardará evidencia.

7.1.19 Seguridad de la información en las relaciones con los proveedores

Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios del proveedor.

Los contratos con los proveedores, de acuerdo a las normativas de FONCODES está sujetos a cláusulas de confidencialidad y no divulgación de la información institucional.

7.1.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores

Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.

El objetivo es asegurar la protección a los activos de FONCODES que son accesibles por proveedores.

Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.

FONCODES exigirá la firma del Acuerdo de Confidencialidad a los proveedores, y colaboradores, para efectos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información, este documento debe ser revisado regularmente y documentado.

En las relaciones con los proveedores se acordará y figurará en los contratos los aspectos de seguridad de información, como cláusulas de confidencialidad, respeto y observancia de la Política de Seguridad de FONCODES.

7.1.21 Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)

Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las TIC.

Se asegurará que la cadena de suministro funcione en caso de incidentes o siniestros, con el fin de dar continuidad a las operaciones de FONCODES.

7.1.22 Seguimiento, revisión y gestión de cambios en servicios de proveedores

La organización debe hacer seguimiento, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.

FONCODES debe monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores; asimismo manejar la gestión de cambios en la provisión de servicios, observando y considerando la criticidad de los servicios prestados, evaluando permanente mente los riegos del proceso.

7.1.23 Seguridad de la información en el uso de servicios en la nube

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.

Considerando:

- Evaluación de Riesgos
- Definición de Políticas y Procedimientos
- Selección de Proveedores de Servicios en la Nube (CSP)
- Implementación de Controles Técnicos
- Capacitación y Concienciación
- Monitoreo y Revisión Continua
- Gestión de Incidentes

7.1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

La organización debe planificar y preparar la gestión de los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, las funciones y las responsabilidades de gestión de incidentes de seguridad de la información.

El objetivo es asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.

Para ello la UTI desarrollará un Procedimiento de Gestión de Incidentes de Seguridad de Información, donde se detallará la planificación, la evaluación, decisión, respuesta y aprendizaje de los incidentes de seguridad (Lecciones Aprendidas).

7.1.25 Evaluación y decisión sobre eventos de seguridad de la información

La organización debe evaluar los eventos de seguridad de la información y decidir si se categorizan como incidentes de seguridad de la información.

Se incluirá en el Procedimiento de Gestión de Incidentes de Seguridad de Información.

7.1.26 Respuesta a incidentes de seguridad de la información

Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Se incluirá en el Procedimiento de Gestión de Incidentes de Seguridad de Información.

7.1.27 Aprendizaje de los incidentes de seguridad de la información

El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.

Se incluirá en el Procedimiento de Gestión de Incidentes de Seguridad de Información, la extracción de lecciones aprendidas y se sociabilizará con las personas involucradas.

7.1.28 Recolección de evidencia

FONCODES deberá establecer e implementar un procedimiento para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

Establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia, es esencial para responder eficazmente a los incidentes de seguridad, proteger los activos de FONCODES y mantener la confianza digital.

Este procedimiento permite una detección temprana de amenazas, un análisis forense adecuado, una respuesta rápida y una mejora continua de la postura de seguridad.

7.1.29 Seguridad de la información durante una interrupción

FONCODES tiene planificado cómo mantener la seguridad de la información en un nivel apropiado durante una interrupción, de acuerdo al “Plan de Recuperación de los Servicios de la Tecnología de la Información”.

7.1.30 Preparación de las TIC para la continuidad del negocio

La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

La UTI adecuará sus operaciones a los lineamientos de la Resolución Ministerial N° 320-2021-PCM, aprueba los “Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno”.

La UTI, cuenta asimismo con un Plan de Recuperación de los Servicios de la Tecnología de Información, que es un subconjunto de un Plan de Continuidad de Negocio, que contempla como reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión, etc.

Este Plan de Recuperación de los Servicios de la Tecnología de Información - Son procedimientos específicos preestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento particular para el cual se tiene escenarios definidos.

El Plan de Recuperación de los Servicios de la Tecnología de Información para UTI, implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los servicios informáticos, en base a eso de plantean escenarios y de acuerdo a ello se plantean Planes de Acción ante los escenarios que se presenten.

La UTI conceptualiza contingencia, como una situación en la que se interrumpa las operaciones habituales de la institución, o se comprometa fuertemente el nivel de la misma por más tiempo que el definido como admisible (ventana de tolerancia), no pudiéndose solucionar dicha situación aplicando los procedimientos habituales.

FONCODES con Resolución de Dirección Ejecutiva N° 104-2023-FONCODES-DE CSIRT Conformación del Equipo de Respuesta ante Incidentes de Seguridad; creó el Equipo de Respuestas para Afrontar los Incidentes de Seguridad de Información (CSIRT), conformada por servidores civiles de UTI, mayormente.

7.1.31 Requisitos legales, estatutarios, regulatorios y contractuales

Los requisitos legales, estatutarios, regulatorios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. Para lo cual FONCODES lleva actualizada una Base de Datos de las normativas legales y regulatorias que afectan a la UTI:

7.1.32 Derechos de propiedad intelectual

FONCODES tiene implementado procedimientos apropiados para proteger los derechos de propiedad intelectual.

Como por ejemplo concientización por medio de pantallazos de información sobre las normativas que protegen los derechos de propiedad intelectual, revisiones periódicas de software no autorizado, entre otras.

7.1.33 Protección de registros

Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.

Estos logs generados por el sistema operativo y los sistemas existentes, deberán ser activados para su registro y guardados, para evidencias de lo actuado en las operaciones

Las actividades del administrador del sistema, administrador de base de datos, del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.

7.1.34 Privacidad y protección de la información de identificación personal (IIP)

FONCODES debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.

Como por ejemplo concientización por medio de pantallazos de información sobre capacitación de usuarios, en cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales, talleres, charlas, entre otros.

7.1.35 Revisión independiente de la seguridad de la información

El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, procesos y tecnologías, debe revisarse de forma independiente en intervalos planificados o cuando se produzcan cambios significativos.

El objetivo es minimizar las debilidades en el Sistema de Gestión de Seguridad de Información.

UTI debe coordinar con los entes pertinentes (DE y OCI) la auditoria y/o revisión del sistema de seguridad por un ente independiente, a intervalos planificados o cuando ocurra cambios significativos.

7.1.36 Cumplimiento con políticas, reglas y normas de seguridad de la información

Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas específicas, las reglas y las normas.

El objetivo es evitar infracciones a las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de información y a cualquier requisito de seguridad.

Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.

Para ello se guardará en una Base de Datos y se informará sobre la actualización de esta, a la jefatura de UTI.

Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales para evitar caer en incumplimientos legales o administrativos.

7.1.37 Procedimientos operativos documentados

Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

Los procedimientos operativos correspondientes a seguridad de información serán documentados y puestos a disposición de todos los usuarios a través de medios digitales.

7.2 Controles de personal

7.2.1 Selección

Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables,

y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos percibidos.

La URH y la UTI deben establecer la clasificación de la información a la que tendrá acceso el/la servidor/a del FONCODES, esto conforme a los riesgos percibidos.

Asimismo, la URH deberá verificar los antecedentes de todos los candidatos a ser empleados en concordancia con las leyes, regulaciones y ética relevantes.

7.2.2 Términos y condiciones del empleo

Los acuerdos contractuales con servidores y proveedores deben estipular responsabilidades de éstos y de la organización, respecto de la seguridad de la información.

La Alta Dirección debe instruir sobre los requisitos de seguridad normados en FONCODES, tanto a los servidores como a otras personas que presten servicios a la institución.

La capacitación en seguridad de información a los/las servidores/as debe ser constante, coordinándose esta entre la UTI y la Unidad de Recursos Humanos. En el caso de los contratistas, la capacitación la realiza la UTI en coordinación con la UA.

7.2.3 Toma de conciencia, educación y entrenamiento sobre la seguridad de la información

El servidor civil de la organización y las partes interesadas pertinentes deben recibir una adecuada concientización, educación y capacitación en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos, según sea pertinente para su función laboral.

La UTI en coordinación con URH capacita a todos los/las servidores/as de la entidad sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen. En el caso de los contratistas se realiza en coordinación con la UA.

FONCODES debe requerir a todos los servidores civiles la aplicación de la seguridad de la información en concordancia con las políticas y normativas establecidas por la institución, y alineadas con las normas sectoriales al respecto. En el caso de los contratistas se realiza en coordinación de la UTI con la UA.

7.2.4 Proceso disciplinario

Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el servidor y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.

En caso de los servidores civiles, la URH remite a la secretaria técnica de Procesos Disciplinarios la información sobre posibles infracciones a la seguridad de la información.

7.2.5 Responsabilidades después del cese o cambio de empleo

Las responsabilidades y obligaciones en materia de seguridad de la información que siguen siendo válidos después del cese o cambio de empleo deben definirse, aplicarse y comunicarse al servidor pertinente y otras partes interesadas.

La URH es responsable de informar a la UTI sobre las desvinculaciones o cambios de los servidores civiles del FONCODES, tal como se encuentra establecido en el “Procedimiento de Gestión de cuentas de usuario”.

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al colaborador o contratista y asegurar su cumplimiento.

7.2.6 Acuerdos de confidencialidad o no divulgación

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.

7.2.7 Trabajo remoto

Se debe implementar medidas de seguridad cuando el servidor civil trabaja de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.

Para la modalidad trabajo remoto, la URH debe informar a la UTI sobre los servidores civiles que harán dicha modalidad de trabajo previo requerimiento del Jefe inmediato, con ello la UTI habilita los accesos de usuario.

Cuando se desarrolle el trabajo remoto, los/las servidores/as pueden solicitar que se le otorgue un equipo para trabajo desde casa o desde la ubicación remota autorizada, siempre y cuando se cuente con disponibilidad y autorización del Jefe de la Unidad de Organización, para ello, deberá coordinar la salida o movilización de los bienes asignados conforme lo establecido por la Unidad de Administración.

Los procesos de trabajo remoto deben ser autorizados por la UTI, debiendo ser limitados entre fechas, especificándose el tipo de tareas que debe efectuarse, además de señalar los riesgos que ello implica.

7.2.8 Reporte de eventos de seguridad de la información

La organización debe proporcionar un mecanismo para que el servidor civil informe eventos de seguridad de la información observados o bajo sospecha a través de los canales apropiados de manera oportuna.

Los reportes de eventos de seguridad de información deben ser reportados y guardados para efectos de dejar evidencias para el control pertinente.

7.3 Controles físicos

7.3.1 Perímetros de seguridad física

Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

El objetivo es impedir que el acceso físico no autorizado, pueda causar daño e interferencia a la información y a las instalaciones de procesamiento de la información de FONCODES.

Los perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.

7.3.2 Ingreso físico

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.

El datacenter institucional, está protegido con dispositivos biométricos, y medidas y procedimientos que impiden que personas no autorizadas ingresen a sus instalaciones.

Asimismo, se encuentra restringido el ingreso a los espacios de soporte de sistemas, producción y desarrollo. Así como al Datacenter, que tendrá control de acceso por medio de dispositivos biométricos.

7.3.3 Asegurar oficinas, salas e instalaciones

Se debe tener protección para garantizar la seguridad física de las áreas y oficinas, con extintores y equipos de luces de emergencia, así como zonas seguras y vías de escape ante emergencias. Garantizando así el trabajo en áreas seguras.

7.3.4 Supervisión de la seguridad física

Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

Se utilizará cámaras web y sensores para monitorear las instalaciones críticas.

7.3.5 Protección contra amenazas físicas y ambientales

Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

La institución tendrá vigilancia en sótanos y áreas de carga y descarga de bultos u equipos.

7.3.6 Trabajo en áreas seguras

Deben diseñarse e implementarse medidas de seguridad para trabajar en áreas seguras.

La seguridad física para oficinas, áreas e instalaciones está asegurada por puertas, que fuera de las horas de oficina deben estar cerradas y se contará además con vigilancia privada que debe ser instruida sobre temas de seguridad de información.

Asimismo, todo equipo informático, debe ser protegido contra riesgos y amenazas de falta de energía eléctrica, fallas de señal de internet, así como accidentes más comunes.

En cuanto a la seguridad del servidor civil se coordinará con RRHH y los encargados de Seguridad y Salud en el trabajo.

7.3.7 Escritorio y pantalla limpios

Todo usuario debe tener su escritorio limpio de papeles y medios de almacenamiento removibles, así como mantener su pantalla limpia para asegurar un funcionamiento adecuado de sus equipos.

7.3.8 Ubicación y protección de los equipos

Los equipos deben estar ubicados de forma segura y protegidos.

Asimismo, todo equipo informático, debe ser protegido contra riesgos y amenazas de falta de energía eléctrica, fallas de señal de internet, así como accidentes más comunes.

7.3.9 Seguridad de los activos fuera de las instalaciones

Los activos fuera del sitio deben protegerse.

Los equipos informáticos que, por necesidad de trabajo, deban llevarse fuera de los locales de FONCODES, deben ser debidamente autorizados por la Jefatura correspondiente, por la Coordinación de Logística y comunicado a la UTI.

7.3.10 Medios de almacenamiento

Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación.

FONCODES deberá gestionar durante su ciclo de vida útil, disponer o reutilizar de una forma segura los equipos, para ello los medios de almacenamiento de estos serán revisados, de tal manera que el software o licencia se haya eliminado o sobrescrito de manera segura antes de su disposición o reutilización.

7.3.11 Servicios de suministro de apoyo

Las instalaciones de procesamiento de información deben protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios de suministro de apoyo.

FONCODES contará con sistemas de protección ante cortes de energía eléctrica, sistemas UPS y apoyo de grupo electrógeno para cuando ocurran cortes de energía eléctrica.

7.3.12 Seguridad del cableado

Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra interceptaciones, interferencias o daños.

El cableado de red y eléctrico, deben estar debidamente acondicionados para garantizar la correcta transmisión de la señal y evitar accidentes.

7.3.13 Mantenimiento de equipos

El equipo debe mantenerse correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.

La UTI para las instalaciones de la Sede Central y los responsables de las demás Sedes y las UTS, son responsables de coordinar y gestionar el mantenimiento de los equipos informáticos y sus instalaciones para la seguridad de ellos, para garantizar la continuidad de las operaciones.

7.3.14 Eliminación segura o reutilización de equipos

Los elementos del equipo que contienen medios de almacenamiento deben verificarse para asegurar que los datos sensibles y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

FONCODES a través de UTI, debe elaborar un informe técnico y disponer con el Coordinador de Logística, para dar de baja los medios de manera segura cuando ya no sean aptos para su uso, utilizando procedimientos formales.

7.4 Controles tecnológicos

7.4.1 Dispositivos terminales del usuario

La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debe protegerse.

Se dispondrá de backups (Ver 7.4.13 Copia de seguridad de la información).

Protectores de pantalla para información confidencial y niveles de acceso a la data según corresponda.

7.4.2 Derechos de acceso privilegiados

La asignación y el uso de derechos de acceso privilegiado deben restringirse y administrarse.

Los accesos privilegiados solo proceden con autorización de la Jefatura de UTI y se guardará un control constante de quienes lo poseen.

7.4.3 Restricción de acceso a la información

El acceso a la información y otros activos asociados debe restringirse de acuerdo con la política específica establecida sobre control de acceso.

Toda aplicación informática de FONCODES, deberá tener un sistema de seguridad que restrinja el acceso a usuarios no autorizados.

Todos los accesos a sistemas o a aplicaciones, deberán antes de ingresar a estos, registrase con su usuario y su clave de usuario autorizado para esos sistemas u aplicativos.

La UTI definirá perfiles de acceso al sistema y aplicaciones, los cuales estarán establecidos por la jerarquía del servidor civil, así como las funciones que desempeña y a solicitud de los Jefes de Unidad o Coordinadores.

7.4.4 Acceso al código fuente

El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las librerías de software debe administrarse adecuadamente.

La UTI, luego de haber culminado el desarrollo o adquisición del aplicativo informático, es el encargado de la custodia de los programas fuente y documentación generada a partir de su desarrollo o adquisición, así como de velar por su correcto funcionamiento. Por lo tanto, quienes hagan uso del aplicativo informático (usuarios) son responsables de toda la información y/o documentación que se registre o procese.

7.4.5 Autenticación segura

Se deben implementar tecnologías y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política específica sobre el control de acceso.

Toda aplicación informática de FONCODES, deberá tener un sistema de seguridad que restrinja el acceso a usuarios no autorizados, es decir una autentificación segura.

Todos los accesos a sistemas o a aplicaciones, deberán antes de ingresar a estos, registrase con su usuario y su clave de usuario autorizado para esos sistemas u aplicativos.

La UTI evaluará en algunos casos usar más de una autentificación considerando:

Autentificación multifactor (MFA) o biometría.

7.4.6 Gestión de capacidad

El uso de recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.

La gestión de la capacidad, se debe monitorear, afinar el uso de los recursos, así como realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema, tal como se explica a continuación:

Se debe aplicar el monitoreo de los sistemas con el fin de asegurar, y donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

Se deben instalar controles para la detección de problemas en un tiempo prudencial.

Las proyecciones, deben tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en FONCODES.

7.4.7 Protección contra programas maliciosos (malware)

La protección contra programas maliciosos (malware) debe implementarse y respaldarse mediante la toma de conciencia adecuada del usuario.

El objetivo es asegurar que la información y las instalaciones de procesamiento de la información Esten protegidas contra códigos maliciosos.

La UTI debe desarrollar controles de detección, prevención y recuperación para proteger contra códigos maliciosos y estos deben ser implementados, en combinación con una concientización apropiada de los usuarios.

Estando prohibido que códigos extraños sean ejecutados por personas no autorizadas, y ajenas al servidor civil de UTI.

7.4.8 Gestión de vulnerabilidades técnicas

Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.

La Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.

La UTI revisará los riesgos de seguridad de la información de la entidad y coordinar la elaboración de los planes de tratamiento, en coordinación con las y los responsables de los órganos y la Unidad de Planeamiento, Presupuesto y Modernización en su calidad de órgano técnico en la implementación de la gestión de riesgos.

7.4.9 Gestión de la configuración

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

La gestión de la configuración es un proceso sistemático para asegurar que el hardware, software, servicios y redes de FONCODES operen de manera segura y eficiente. Implica establecer, mantener y controlar las configuraciones de los sistemas de TI para minimizar las vulnerabilidades y garantizar el cumplimiento de las políticas y estándares de seguridad.

Configuraciones de seguridad: FONCODES establecerá una configuración base para todos los servidores informáticos que ejecutan aplicaciones web. Esta configuración incluye:

Firewall activado y configurado para permitir solo el tráfico necesario.

Autenticación habilitada para todos los usuarios con acceso administrativo.

Análisis regulares de vulnerabilidades y aplicación automática de parches de seguridad.

Registro centralizado de eventos de seguridad para su monitoreo y análisis.

Hardware: Para los equipos portátiles de los empleados, la política de gestión de configuración puede especificar:

Requerir una contraseña compleja para el inicio de sesión.

Instalación y actualización automática de software antivirus.

Software: La gestión de la configuración asegura que las aplicaciones estén actualizadas y configuradas de forma segura.

Configurar las aplicaciones para que utilicen los ajustes de seguridad más restrictivos por defecto.

Implementar controles para evitar la instalación de software no autorizado por los usuarios.

Servicios: Para los servicios TIC que utiliza la empresa, la gestión de la configuración podría incluir:

Configurar el acceso a los servicios con el principio de mínimo privilegio, dando a cada usuario solo los permisos necesarios para realizar su trabajo.

Activar el registro de auditoría para rastrear todas las acciones realizadas en los servicios en la nube.

Redes: La gestión de la configuración de la red implica:

Configurar los routers y switches con contraseñas seguras y actualizadas.

Implementar un sistema de detección de intrusiones (IDS) para monitorear el tráfico de la red en busca de actividades sospechosas.

Deshabilitar los servicios y puertos innecesarios en los dispositivos de red.

7.4.10 Eliminación de información

La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.

Cuando se requiera eliminar la información contenida en un medio informático removible se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que, no permitan la recuperación de los datos.

El técnico de la UTI coordinará con el titular del banco de datos personales sobre la información a eliminar, contenida en los medios informáticos removibles.

Seguridad en la copia o reproducción de documentos.

Cuando sea necesario, el titular del banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales.

Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales:

a) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.

b) Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.

c) Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.

d) Procedimiento de control de procesos en el manejo de datos personales.

e) Se procederá a revisar como mínimo una vez al semestre los accesos realizados a los datos personales en base a los registros de auditoría de la base de datos.

Contemplando:

- ¿Quiénes tienen acceso a los datos personales?
- ¿Quiénes hacen accesos a los datos personales?
- ¿Qué operaciones se efectúan con los datos personales?

7.4.11 Enmascaramiento de datos

El enmascaramiento de datos debe utilizarse de acuerdo con la política específica de la organización sobre control de acceso, otras políticas específicas relacionadas y los requisitos del negocio, teniendo en cuenta la legislación aplicable.

FONCODES utilizara enmascaramiento de datos, como técnica de seguridad para proteger la información sensible reemplazándola con datos ficticios, pero con un formato similar al original. El objetivo principal es salvaguardar la información confidencial y privada, especialmente cuando se comparte con terceros para fines como pruebas de software o capacitación de usuarios, en cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales.

7.4.12 Prevención de fuga de datos

Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y otros dispositivos que procesan, almacenan o transmiten información sensible.

Para prevenir la fuga de datos de la Red Informática de FONCODES (exposición accidental o intencional de información sensible a partes no autorizadas). Se implementarán las siguientes medidas.

Firewalls: Actúan como la primera línea de defensa, filtrando el tráfico de red y bloqueando accesos no autorizados. El firewall está configurado para permitir solo las comunicaciones autorizadas.

Políticas de acceso y control de dispositivos: Se establecen políticas de acceso estrictas, basadas en el principio de mínimo privilegio, donde cada usuario solo tiene acceso a la información necesaria para realizar su trabajo.

Actualizaciones y gestión de vulnerabilidades: Se revisan las versiones de software para evitar el ingreso de intrusos.

7.4.13 Copia de seguridad de la información

El objetivo es protegerse contra la pérdida de datos.

Las copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.

El usuario es responsable de almacenar y realizar el respaldo de sus archivos de trabajo electrónicamente, de requerirlo podrá solicitar el apoyo técnico de la UTI.

En el caso de los Unidades Territoriales, el Jefe de la Unidad Territorial (JUD), es el responsable que frecuentemente se generen las copias de respaldo (backup) de los archivos electrónicos críticos que son almacenados en el equipo- servidor informático de la Unidad Territorial, asimismo de todos aquellos documentos electrónicos que por su importancia deben almacenarse con la protección que el caso amerita. En este punto la UTI podrá orientar en el proceso.

Como medida de prevención se recomienda que regularmente se haga la remisión de las copias de respaldo de las Unidades Territoriales hacia la UTI.

En el caso de la Sede Central las copias de respaldo (backups) del equipo-servidor informático, son realizados por la UTI.

7.4.14 Redundancia de las instalaciones de procesamiento de información

Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.

El objetivo es asegurar la disponibilidad de las instalaciones y procesamiento de la información, ante diferentes contingencias.

La UTI hará las gestiones necesarias para que FONCODES cuente con un Site Alterno y en lo posible para asegurar la Continuidad Operativa.

7.4.15 Registro

Se deben producir, almacenar, proteger y analizar los registros que guarden actividades, excepciones, fallas y otros eventos relevantes.

Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.

7.4.16 Actividades de monitoreo

Las redes, los sistemas y las aplicaciones serán monitoreadas para detectar comportamientos anómalos y tomar acciones para evaluar posibles incidentes de seguridad de la información.

Cuando menos semestralmente, se emitirá un Informe de vulnerabilidades en el cual debe figurar, monitoreo de software no autorizado, eventos anómalos en los usuarios, posibles vulnerabilidades, etc.

7.4.17 Sincronización de reloj

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de FONCODES, se deben sincronizar con una fuente que proporcione la hora exacta acordada.

7.4.18 Uso de programas de utilidad privilegiados

Se debe restringir y controlar estrictamente el uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones.

El uso de programas de servicio (utilitarios) que pueden eludir las medidas de control del sistema y de las aplicaciones, deben ser de uso exclusivo de la UTI, salvo su autorización temporal, considerándose como una transgresión a la seguridad de la información su uso no autorizado.

7.4.19 Instalación de software en sistemas operativos

Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos.

La UTI implementará controles para evitar la instalación de software en la red de FONCODES.

Todo archivo que provenga de un origen desconocido o sospechoso a través de un medio magnético, de Internet o adjunto a un correo electrónico, debe ser revisado previamente por el programa de antivirus provisto por la institución.

7.4.20 Seguridad de redes

Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en sistemas y aplicaciones.

La red de FONCODES será gestionada y controlada para proteger la información en los sistemas y las aplicaciones.

La solución de seguridad perimetral implementada, evita la recepción de correos no deseados, así como la suplantación de identidad de los correos institucionales.

La solución antivirus implementado evitará la propagación de virus informáticos y sus variantes a través de este medio de comunicación.

7.4.21 Seguridad de servicios de red

Deben identificarse, implementarse y monitorearse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

FONCODES cuenta con mecanismos de seguridad perimetral contratada a un proveedor externo.

Los servicios de red son identificados y protegidos a nivel nacional.

7.4.22 Segregación de redes

Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes, para mayor seguridad, tal como con el uso de las VLANs. (red de área local virtual, que es un método para crear redes lógicas independientes dentro de una misma red física).

7.4.23 Filtrado de la web

El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.

FONCODES la técnica de filtrado de red para controlar el flujo de datos hacia y desde una red, asegurando que solo el tráfico autorizado pueda acceder a los recursos de la red. Este proceso se basa en la revisión de paquetes de datos y la aplicación de reglas predefinidas para determinar qué tráfico se permite y cuál se bloquea.

Dirección IP: FONCODES bloqueará todas las conexiones provenientes de direcciones IP conocidas por ser maliciosas. Si un paquete llega desde una dirección IP en esta lista negra, el firewall lo bloqueará automáticamente.

Puertos: FONCODES solo permite tráfico a través de puertos autorizados.

Protocolo: El firewall estará configurado para permitir solo ciertos protocolos autorizados, y bloquear otros que no sean necesarios para las operaciones diarias.

Contenido: FONCODES bloqueara ciertas direcciones IP que considera no adecuadas.

7.4.24 Uso de criptografía

Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

El objetivo es asegurar el uso apropiado hacer que y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información de FONCODES.

Para efectos de los controles criptográficos, FONCODES se basará en el documento Sectorial “Lineamientos de la Seguridad de Información del Ministerio de Desarrollo e Inclusión Social”.

7.4.25 Ciclo de vida de desarrollo seguro

Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

Todos los requisitos relevantes de seguridad de la información son establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización, en concordancia con los criterios de aceptación de los nuevos sistemas y todo lo relacionado con adquisición, desarrollo y mantenimiento de sistemas se rige por la Norma Técnica Peruana NTP-ISO/IEC 12207:2016, Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software 3ª Edición” .

FONCODES se alineará en temas desarrollo de software a la denominada” Directiva de Procedimientos del Ciclo de Vida del Software del Ministerio de Desarrollo e Inclusión Social”, con el fin de tener un software seguro.

7.4.26 Requisitos de seguridad de la aplicación

Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

FONCODES tendrá en cuenta los requisitos de seguridad de la información, que deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

- En especial los principios básicos de ingeniería de sistemas seguros como:
- Seguridad desde el diseño del software
- Principio de menor privilegio (solo permisos necesarios)
- Defensa en profundidad (Implementar múltiples capas de seguridad)
- Auditoría y monitoreo para detectar anomalías.
- Actualización y parches (tener actualizadas las versiones de software).
- Cifrado de datos para proteger la información sensible.
- Pruebas de seguridad a intervalos regulares a lo largo del ciclo de vida.
- Conciencia y formación (educar a usuarios sobre las mejores prácticas).
- Gestión de incidentes (dado en el Plan de Continuidad Operativa).
- Documentación de aplicativos y cumplimiento de normas de seguridad.

7.4.27 Arquitectura de sistemas seguros y principios de ingeniería

Los principios de ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistema de información.

La arquitectura de sistemas seguros se refiere al diseño y estructuración de sistemas informáticos que integran medidas de seguridad desde su concepción. Esto implica considerar no solo la funcionalidad del sistema, sino también su resistencia a amenazas y vulnerabilidades. Los principios de ingeniería en este contexto son guías que ayudan a crear sistemas robustos y seguros, tales como:

Principio del Mínimo Privilegio

Cada componente del sistema, así como cada usuario, debe tener solo los permisos necesarios para realizar sus funciones

Defensa en Profundidad

La arquitectura incluye múltiples capas de seguridad, como:

Cortafuegos: Se utilizan para filtrar el tráfico no autorizado hacia la aplicación.

Sistemas de Detección y Respuesta ante Intrusiones (EDR): Monitorean el comportamiento del sistema para detectar actividades sospechosas.

Cifrado: Todos los datos sensibles se cifran tanto en reposo como en tránsito, asegurando que incluso si los datos son interceptados, no sean legibles sin las claves adecuadas.

Modelado de Amenazas

Antes de implementar el sistema, se realiza un análisis exhaustivo para identificar posibles vulnerabilidades. Se crean escenarios hipotéticos sobre cómo un atacante podría comprometer el sistema y se diseñan contramedidas adecuadas.

Separación de Funciones

Para evitar que una sola persona tenga control total sobre un proceso crítico (como la gestión de pagos), se implementa un sistema donde diferentes usuarios deben colaborar para completar ciertas acciones.

Auditoría y Monitoreo Continuo

Se establecen procesos para registrar todas las acciones realizadas en el sistema y se revisan regularmente para detectar comportamientos anómalos o no autorizados. Esto permite a la empresa reaccionar rápidamente ante incidentes potenciales y mejorar continuamente sus medidas de seguridad.

7.4.28 Codificación segura

FONCODES aplica los principios de codificación segura al desarrollo de software.

FONCODES conceptualiza la codificación segura, como la práctica de desarrollar software de manera que se minimicen las vulnerabilidades y se protejan los datos sensibles. Implica aplicar estándares y buenas prácticas durante el proceso de desarrollo para prevenir ataques cibernéticos y asegurar la integridad de la aplicación.

Algunos puntos que considera:

- Validación de entrada de datos
- Autenticación y gestión de contraseñas
- Control de acceso
- Mantenerlo simple
- Prácticas criptográficas
- Gestión de errores y registros
- Protección de datos
- Modelado de amenazas

7.4.29 Pruebas de seguridad en desarrollo y aceptación.

Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

Las pruebas de seguridad en el desarrollo y aceptación de software son procesos críticos para identificar vulnerabilidades y garantizar que las aplicaciones sean resistentes a las ciberamenazas. Estas pruebas se realizan en diferentes etapas del ciclo de vida del desarrollo de software (SDLC) para minimizar los riesgos y proteger los activos digitales.

Algunas pruebas a efectuar:

- Análisis de código estático (SAST)
- Pruebas de penetración (pentesting)
- Pruebas de seguridad dinámicas (DAST)
- Vulnerabilidades que puedan ser explotadas1.

7.4.30 Desarrollo subcontratado

La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

FONCODES a través de la UTI, dirigirá, monitoreará y revisará las actividades relacionadas con el desarrollo de sistemas subcontratados por proveedores externos.

7.4.31 Separación de los entornos de desarrollo, prueba y producción

Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.

Las áreas encargadas del desarrollo de sistemas, de producción y calidad, están segregadas en sus funciones, para prevenir modificaciones no autorizadas, paradas o mal uso de los activos de la institución.

7.4.32 Gestión de cambios

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

El proceso de gestión de cambios en FONCODES, está formado por seis actividades principales, según se indica continuación;

- Identificar los cambios potenciales;
- Analizar la solicitud de cambios;
- Evaluar cambios;
- Planificar cambios;
- Implementar cambios; y
- Revisar y finalizar el proceso de cambios.

Asimismo, se conducen los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta el grado crítico de los sistemas y los procesos de la entidad involucrados y la reevaluación de los riesgos.

7.4.33 Información de las pruebas

La información de las pruebas, FONCODES las selecciona, protege y gestiona adecuadamente.

La protección de la información durante las pruebas de software es crucial para garantizar la seguridad de los sistemas y la integridad de los datos, evitando las filtraciones de datos que pueden ocurrir si las pruebas no se realizan con las debidas precauciones.

Algunas técnicas utilizadas:

- Uso de Datos Sintéticos: En lugar de utilizar datos reales, se generan datos sintéticos que simulan condiciones reales sin comprometer información sensible.
- Acceso Controlado: Limitar el acceso al entorno de pruebas solo a servidores civiles autorizados y utilizar autenticación robusta para proteger los sistemas.
- Pruebas Regulares de Seguridad: Realizar pruebas periódicas para identificar y corregir vulnerabilidades antes del lanzamiento del software.

7.4.34 Protección de los sistemas de información durante las pruebas de auditoría

Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos son planificadas y se acuerdan entre el evaluador y la UTI. Este proceso asegura que se aborden adecuadamente los

riesgos y se evalúen los controles existentes en el entorno tecnológico, asegurando así la continuidad operativa.

8. **DISPOSICIONES COMPLEMENTARIAS**

8.1 Todos aquellos aspectos en materia de Tecnologías de la Información que no se hayan contemplado en la presente Directiva, serán resueltos por la UTI.

8.2 Toda excepción a la presente norma en aspectos relacionados con las Tecnologías de la Información, debe ser resuelta y aprobada por la UTI.

8.3 La UTI establece las políticas de seguridad necesarias para el buen uso de los activos y servicios informáticos.

8.4 Todos los requerimientos de servicios informáticos deben ser solicitados a la UTI a través de los mecanismos indicados en el Procedimiento N° 122-2020- FONCODES/UTI: "Gestión de Solicitudes de Atención a usuarios de Servicios de Tecnologías de la Información".

8.5 Todos los requerimientos de desarrollo de soluciones informáticas deben ser solicitados a la UTI conforme lo establecido en el Procedimiento N° 113-2020- FONCODES/UTI: "Desarrollo, Operación, Mantenimiento y Retiro de Productos de Software".

9. **PROCESO RELACIONADO**

   S01 Gestión de las Tecnologías de la Información

10. **ANEXO**

SIGLAS O ABREVIATURAS (ACRONOMINOS)

ACRÓNIMO	D E N O M I N A C I O N
FONCODES	Fondo de Cooperación para el Desarrollo Social
SGSI	Sistema de Gestión de la Seguridad de la Información
ANS o SLA	Acuerdo de Nivel de Servicio o Service Level Agreement
CPU	Unidad Central de Proceso
DVD	Digital Versatile Disc
FTP	File Transfer Protocol
ISO	Organización Internacional de Normalización (Del Ingles: International Organization For Standardization)
IEC	Comisión Electrotécnica Internacional
NTP	Norma Técnica Peruana
OWA	Outlook Web Access
RIS	Reglamento Interno del Servidor
SGTD	Secretaría de Gobierno y Transformación Digital
TI	Tecnologías de la Información
DE	Dirección Ejecutiva
OCI	Órgano de Control Institucional
UA	Unidad de Administración
URH	Unidad de Recursos Humanos
UT	Unidad Territorial
UTI	Unidad de Tecnologías de la Información
CSIRT	Computer Security Incident Response Team. El Equipo de Respuesta de Incidentes de Seguridad Informática del Perú
OWASP	Open Web Application Security Project. (En español 'Proyecto abierto de seguridad de aplicaciones web')
NIST	National Institute of Standards and Technology (Instituto Nacional de e Estándares y Tecnología).