



FONDO SOLIDARIO PARA LA SALUD

Manual de Confidencialidad

2024

UNIDAD DE PLANIFICACIÓN



FONDO SOLIDARIO PARA LA SALUD

El Infrascrito secretario del Consejo Directivo del Fondo Solidario para la Salud, **CERTIFICA:** Que en el Libro de Actas de Consejo Directivo que esta Institución lleva se encuentra asentada el Acta Ordinaria número **CIENTO TREINTA Y SEIS** correspondiente a la sesión de Consejo Directivo, celebrada a las ocho horas, del día veintiocho de febrero del año dos mil veinticuatro, en la cual se encuentra asentado el punto que literalmente dice:

6. APROBACIÓN DE MANUAL DE CONFIDENCIALIDAD 2024.

El Director Ejecutivo, presenta a los miembros del Consejo Directivo asistentes para su aprobación el Manual de Confidencialidad año 2024.

Este nuevo manual refuerza el compromiso ético y legal que todos los empleados de la institución deben asumir para la protección de la información de Fosalud.

Sigue manifestando el Director Ejecutivo que mediante la emisión de este instrumento se da cumplimiento a las Normas técnicas de control interno, reforzando el tema de confidencialidad y todo lo relacionado a la seguridad de información que es gestionada por la UTI a través del documento denominado "Guía técnica Unidad Tecnologías de la Información"

Asimismo, con la aprobación de ese manual, se desvanece la observación de la Auditoría Externa Integral 2020 – 2021, la cual menciona que "La institución carece de política, manuales de confidencialidad."

Por las razones antes expuestas se somete a consideración del Consejo Directivo la aprobación del Manual de Confidencialidad 2024.

Por decisión unánime de los miembros del Consejo Directivo asistentes se aprueba el Manual de Confidencialidad 2024 de conformidad a lo antes expuesto.

Por lo que no teniendo nada más que hacer constar al respecto, se extiende la presente en la ciudad de San Salvador, a los veintiocho días del mes de febrero del año dos mil veinticuatro.

Dr. Carlos Emilio Núñez Sandoval
Secretario del Consejo Directivo
Fondo Solidario para la Salud



Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				



FONDO SOLIDARIO PARA LA SALUD

Manual de Confidencialidad

San Salvador, Febrero 2024

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Ficha Catalográfica

2024 – Fondo Solidario para la Salud, Fosalud.

Todos los derechos reservados. Está permitida la reproducción parcial o total de esta obra, siempre que se cite la fuente y que no sea para la venta u otro fin de carácter comercial.

Es responsabilidad de los autores técnicos de este documento, tanto su contenido como los cuadros, diagramas e imágenes.

La documentación oficial del Fosalud, puede ser consultada a través de: <http://www.fosalud.gob.sv>.

1ª Edición, 2024.

Elaboración y emisión:

Fondo Solidario para la Salud, FOSALUD

Unidad de Planificación - UPLAN

9ª Calle Pte. No. 3843, Colonia Escalón, San Salvador

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Contenido

Introducción	3
Objetivos	3
General	3
Específicos.....	3
Base Legal.....	4
Alcance.....	4
Definiciones	4
Información confidencial	6
Responsabilidades.....	6
Procedimiento de manejo de información.....	7
Seguridad de la información.....	8
Sanciones	10
Disposiciones finales.....	10
Revisión y actualización	10
Vigencia.....	10

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

El honorable Consejo directivo del Fondo Solidario para la Salud,

Considerando:

- I. Que de conformidad al Decreto Legislativo número 538 de fecha diecisiete de diciembre de dos mil cuatro, se crea el Fondo Solidario Para la Salud, como una entidad de derecho público, de carácter técnico, de utilidad pública, de duración indefinida y con personalidad jurídica y patrimonio propio, con plena autonomía en el ejercicio de sus funciones, tanto en lo financiero como en lo administrativo y presupuestario, el cual estará adscrito al Ministerio de Salud Pública, con el fin de Conservar la Salud Pública y la Asistencia Social, así como la atención de urgencias y emergencias médicas en todos sus aspectos;
- II. Que el artículo 9 letras d) y g) del Reglamento de la Ley Especial para la Constitución del Fondo Solidario para la Salud establece que es atribución del Consejo Directivo "Aprobar los Manuales necesarios para el funcionamiento del Fosalud", así como "evaluar periódicamente el cumplimiento de los objetivos del Fosalud";
- III. Que de conformidad al artículo 12 del Reglamento de Normas Técnicas de Control Interno Específicas del Fosalud, establece que la Dirección Ejecutiva a través de sus unidades evaluará periódicamente su marco normativo revisando y actualizando los manuales, políticas y procedimientos para asegurarse que contribuyan al logro de sus objetivos institucionales y se adecue al marco legal, caso contrario ordenará los ajustes necesarios;

Por tanto,

En uso de las atribuciones, ACUERDA emitir el siguiente:

MANUAL DE CONFIDENCIALIDAD DEL FOSALUD

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Introducción

En un mundo digitalizado y altamente conectado, la información es uno de los activos más valiosos. La protección de esta información no solo es una responsabilidad institucional, sino también un compromiso ético y legal que todos los miembros de la institución deben asumir.

Cada empleado en el Fondo Solidario para la Salud (Fosalud), debe conocer las normas sobre manejo de información, de modo que las actividades institucionales sean realizadas en acuerdo con la normativa establecida, evitando el conflicto de interés o su manejo inapropiado.

Se reconoce que la confidencialidad es un pilar fundamental y esencial para mantener la confianza de nuestros usuarios y empleados por lo que este manual proporciona una guía sobre cómo identificar, manejar y proteger la información en todos los aspectos de las funciones institucionales. Partiendo de los datos personales de los usuarios, empleados hasta la gestión estratégica de Fosalud, cada forma de información merece un cuidado especial.

Se revisará y actualizará cada dos años para reflejar los cambios en las tecnologías, regulaciones y prácticas que afectan la confidencialidad de la información.

La protección de la información confidencial es un compromiso compartido por todos. Al comprender y adherirse a la normativa establecida en este manual, estamos fortaleciendo la integridad de la institución.

Objetivos

General

Establecer los lineamientos necesarios para proteger la información confidencial de la institución.

Específicos

1. Establecer lineamientos para definir la confidencialidad y cómo debe ser protegida contra el acceso no autorizado, divulgación no autorizada, alteración o destrucción.
2. Asegurar el cumplimiento de las leyes y regulaciones con la privacidad y protección de datos, a través de la socialización.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

3. Fomentar una cultura de compromiso a la seguridad institucional para dar la importancia de proteger la información confidencial institucional.

Base Legal

En el desempeño de sus actividades y prestación de servicios, Fosalud se encuentra con diversas obligaciones de reserva de información y confidencialidad respecto a los procesos que se realizan con terceros.

Dada su naturaleza de prestador de servicios, sus funcionarios y empleados se encuentran sujetos a la siguiente normativa:

- (i) Constitución de la República
- (ii) Ley de Acceso a la Información Pública (LAIP)
- (iii) Código de Ética y Conducta institucional.
- (iv) Reglamento Interno de Trabajo.
- (v) Norma técnica para la conformación, custodia y consulta de expediente clínico.
- (vi) Lineamientos técnicos para el cumplimiento del secreto profesional en el Sistema Nacional Integrado de Salud.
- (vii) Lineamientos emitidos por la Unidad de Documentos y Archivos de Fosalud

Alcance

El presente manual se aplicará a todas las trabajadoras y los trabajadores del Fosalud, que genere o tenga acceso a información confidencial en virtud de su cargo.

Definiciones

A continuación, se detallan las principales definiciones que se utilizarán para este manual:

Confidencialidad: se refiere a la protección de la información contra accesos no autorizados. Incluyendo el control de acceso a la información sensible mediante la autenticación, la autorización y el cifrado de datos para prevenir el acceso no autorizado.

Integridad: se refiere a la precisión y la confiabilidad de la información. La seguridad de la información debe garantizar que la información no sea modificada, dañada o alterada de manera no autorizada, tanto durante el almacenamiento como durante la transmisión.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Disponibilidad: se refiere a garantizar que la información esté disponible y accesible cuando sea necesario para los usuarios autorizados. Esto implica proteger los sistemas y recursos de información contra interrupciones y ataques que puedan afectar la misma.

Autenticación y autorización: Los sistemas de seguridad de la información deben incluir mecanismos de autenticación para verificar la identidad de los usuarios y mecanismos de autorización para determinar cuáles recursos y datos pueden acceder los usuarios autorizados.

Cifrado de datos: es una técnica que se utiliza para proteger la información confidencial mediante la conversión de datos en un formato ilegible que solo puede ser decodificado por usuarios autorizados que poseen la clave de cifrado.

Gestión de accesos privilegiados: implica controlar y monitorear los privilegios de acceso de los usuarios con altos niveles de autoridad dentro de una organización para evitar abusos o accesos no autorizados a información sensible.

Por otra parte, se retoman algunas definiciones detalladas en el artículo 6 de la LAIP:

Datos personales: la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra análoga.

Datos personales sensibles: los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Información confidencial: es aquella información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal debido a un interés personal jurídicamente protegido.

Servidor Público: Persona natural que presta servicios ocasional o permanentemente, remunerados o ad honórem, que ejerzan su cargo por elección, nombramiento, contrato u otra modalidad dentro de la administración del Estado, de los municipios y de las entidades oficiales autónomas sin excepción. Asimismo, comprende a los funcionarios y empleados públicos y agentes de autoridad en todos sus niveles jerárquicos.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Violación de la confidencialidad: divulgación de datos sensibles, así como los incidentes que tienen como resultado algún tipo de consecuencia observable.

Información confidencial

Para la aplicación del manual de confidencialidad, a continuación, se detalla la información institucional que se considera confidencial:

1. Datos personales de los empleados: nombre, dirección, número telefónico, correo electrónico, número de seguro social.
2. Información financiera de los empleados: Salario, préstamos, descuentos.
3. Evaluaciones de desempeño.
4. Amonestaciones al personal.
5. Procesos sancionatorios.
6. Información de salud de los empleados.
7. Contratos laborales.
8. Procesos de compra, mientras no sea adjudicado y notificado al proveedor.
9. Información de expedientes clínico en los establecimientos de Fosalud.
10. Información de producción digitada en los sistemas estadísticos.
11. Acuerdos en reuniones de cualquier índole.

Responsabilidades

Las responsabilidades de los empleados en relación con la protección de la información institucional son fundamentales para garantizar la seguridad y la integridad de los datos dentro de la institución.

A continuación, se detallan algunas responsabilidades:

Conciencia y formación: Los empleados deben estar en constante actualización institucional para conocer sobre la información confidencial y recibir formación periódica sobre las políticas y procedimientos de seguridad de la información.

Cumplimiento de políticas: Los empleados deben cumplir con todas las políticas y procedimientos establecidos en el manual de confidencialidad y otras directrices relacionadas con la protección de la información confidencial.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Manejo seguro de la información: Es responsabilidad de los empleados manejar la información confidencial de manera segura y adecuada, incluyendo la protección de documentos físicos, contraseñas, datos electrónicos y otros medios de información.

Acceso controlado: Se deberá crear mecanismos de control y autorización para asegurar que las y los trabajadores solo tengan acceso a la información confidencial que sea necesaria para llevar a cabo sus funciones laborales.

Protección de dispositivos y datos: Los empleados deben tomar medidas para proteger los dispositivos y medios de almacenamiento de datos, como computadoras, teléfonos móviles, unidades USB, etc., para prevenir accesos no autorizados.

Comunicación segura: Los empleados deben utilizar los canales legales de comunicación para el intercambio de información confidencial, como el uso de correos electrónicos cifrados o sistemas seguros de mensajería.

Detección y reporte de incidentes: Los empleados deben estar atentos a cualquier actividad sospechosa o violación de la seguridad de la información y reportarla de inmediato a los responsables designados dentro de la institución.

Cumplimiento legal y regulatorio: Los empleados deben cumplir con todas las leyes y regulaciones aplicables relacionadas con la protección de la información confidencial, como la Ley de Acceso a la Información Pública (LAIP), Código de ética y conducta, Reglamento interno de trabajo, entre otras.

Procedimiento de manejo de información

Los procedimientos de manejo de la información son prácticas establecidas para la gestión efectiva y segura de la información en la institución. Estos procedimientos abarcan desde la creación y recolección de datos hasta su almacenamiento, uso, transmisión y disposición final. Algunos procedimientos clave de manejo de la información son los siguientes:

Clasificación de la información:

Cada unidad deberá identificar y clasificar la información en diferentes niveles según su sensibilidad y valor, como información pública, interna, confidencial o altamente confidencial.

Creación y captura de datos:

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Establecer procesos para la creación y captura de datos, incluyendo la definición de formatos estandarizados y la captura de datos relevantes para su identificación y gestión.

Almacenamiento seguro:

Determinar dónde y cómo se almacenará la información, garantizando que se utilicen sistemas y tecnologías seguras, como servidores protegidos con cifrado y control de acceso.

Acceso y control de datos:

Establecer el acceso y control para garantizar que solo las personas autorizadas tengan acceso a la información relevante para sus funciones laborales y que se apliquen mecanismos de autenticación y autorización adecuados.

Uso y divulgación:

Definir quién puede usar y divulgar la información, así como los procedimientos para compartir datos internamente y con partes externas, siempre garantizando la confidencialidad y el cumplimiento de regulaciones y políticas.

Transmisión segura:

Implementar medidas de seguridad para proteger la información durante su transmisión, como el uso de protocolos de cifrado y la firma digital para garantizar la autenticidad e integridad de los datos.

Retención y disposición:

El tiempo que se debe tener para conservar la información y los procedimientos para su eliminación segura se realizará en cumpliendo con las disposiciones legales y regulatorias institucionales.

Seguridad de la información.

Para proteger la información confidencial, es crucial implementar medidas de seguridad física y digital.

Medidas de seguridad física

- Se debe implementar sistemas de control de acceso a las instalaciones tales como sistemas electrónicos de seguridad para limitar la entrada a las instalaciones de la institución.
- Instalación de cámaras de seguridad y sistema de videovigilancia para monitorear las instalaciones.
- Mantener cerraduras seguras y restringir el acceso a áreas sensibles a personal autorizado solamente.
- Almacenar equipos y dispositivos que contienen información confidencial en lugares seguros y protegidos contra robos o daños.
- Utilizar áreas de seguridad para proteger servidores.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Medidas de seguridad digital

- Firewalls y seguridad de red para proteger el acceso no autorizado y ataques cibernéticos.
- Utilizar algoritmos de cifrado para proteger la información mientras se transmite a través de redes y cuando se almacena en dispositivos o servidores.
- Gestión de acceso y contraseñas.
- Mantener actualizados los sistemas operativos, software y aplicaciones con los últimos parches de seguridad para corregir vulnerabilidades.
- Realizar copias de seguridad regulares de la información y almacenarlas en ubicaciones seguras.

Adicionalmente, los procedimientos de autenticación y autorización son los componentes más esenciales de la seguridad de la información ya que garantizan que solo las personas autorizadas puedan acceder a la información confidencial.

Autenticación.

Es el proceso de verificar la identidad de un usuario para garantizar que sea quien dice ser antes de permitirle acceder a los sistemas o recursos de información confidencial.

Algunos métodos de autenticación incluyen:

Contraseñas: El método más común de autenticación, donde los usuarios deben proporcionar una combinación de nombre de usuario y contraseña único.

Autenticación de dos factores o multifactor: Requiere que los usuarios proporcionen dos o más formas de autenticación, como una contraseña combinada con un código generado por una aplicación móvil o enviado por mensaje de texto.

Biometría: Utiliza características físicas o comportamentales únicas de un individuo, como huellas dactilares, reconocimiento facial o escaneo de retina, para verificar la identidad.

Tarjetas inteligentes o tokens de seguridad: Dispositivos físicos que los usuarios deben tener en su posesión para autenticarse, como tarjetas inteligentes que contienen un chip o tokens de seguridad que generan códigos de acceso únicos.

Unidad de Planificación	Clasificación	Código:	UPLAN-MAN06-01-2024	
		Edición	1ª	
		Vigencia:	Febrero 2024	
	Manual de Confidencialidad			
Fondo Solidario para la Salud				

Autorización.

La autorización determina qué recursos o datos puede acceder un usuario una vez que se ha autenticado con éxito. La autorización se basa en los derechos y privilegios asignados a cada usuario o grupo de usuarios dentro de un sistema.

Algunos métodos comunes de autorización incluyen:

Control de acceso basado en roles: Asigna permisos de acceso a los usuarios en función de su función o rol dentro de la organización.

Control de acceso basado en atributos: Asigna permisos de acceso basados en ciertos atributos del usuario, como la ubicación, el departamento o el nivel de seguridad.

Listas de control de acceso: Enumera los usuarios y los recursos a los que tienen acceso permitido o denegado de manera explícita.

Sanciones

La divulgación de información confidencial dará lugar a responsabilidades administrativas y laborales de acuerdo con el Reglamento Interno de Trabajo, sin perjuicio de las sanciones a que sean acreedores de conformidad con las leyes aplicables.

Disposiciones finales

Revisión y actualización

El presente Manual será revisado y actualizado cuando existan cambios o avances en los abordajes relativos sobre información catalogada como reservada y/o confidencial en la legislación, cambios en la estructura orgánica o funcionamiento del Fosalud, o cuando se determine necesario por parte del Director Ejecutivo o el Consejo Directivo.

Vigencia

El presente Manual entrará en vigencia a partir de la fecha de la aprobación y firma de este, por parte del Consejo Directivo del Fosalud.