FOSIS
Ministerio de Desarrollo Social y Familia

Gobierno de Chile

RESOLUCION EXENTA Nº FC-F-00750
MAT: APRUEBA POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRÁFICOS Y GESTIÓN DE CLAVES DEL FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL. SSI-A-8.24
SANTIAGO, **12-11-2024**

VISTOS:

Lo dispuesto en la Ley Nº 18.989, en particular en su Título II sobre el Fondo de Solidaridad e Inversión Social; en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en la Resolución N° 7 de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón; en el Decreto Supremo N° 15, de 28 de abril de 2022, del Ministerio de Desarrollo Social y Familia que nombra el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social y demás antecedentes tenidos a la vista.

CONSIDERANDO:

1. Que, el Fondo de Solidaridad e Inversión Social es un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, cuya finalidad es financiar en todo a parte planes, programas, proyectos y actividades especiales de desarrollo social, los que deberán coordinarse con los que realicen otras reparticiones del Estado.

2. Que, la misión del FOSIS, es "contribuir a la superación de la pobreza y vulnerabilidad social a través de estrategias que fortalezcan la cohesión social, las habilidades y capacidades de personas, familias y comunidades, con pertinencia territorial y enfoque de género".

3. Que, el FOSIS debe realizar la definición de las políticas y la verificación del cumplimiento de las normas y las buenas prácticas relacionadas con la seguridad de la información y ciberseguridad y de los activos de información que les pertenecen.

4. Que, por lo anteriormente señalado, resulta necesario que el FOSIS cuente con una Política para el uso de controles criptográficos y gestión de claves, cuyo objetivo consiste en establecer normas para el uso de algoritmos de encriptación y servicios de protección de información a utilizar en el FOSIS y para el uso, protección y vida útil de las claves criptográficas durante toda su vida útil en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

5. Que, por lo anteriormente señalado, mediante Memorándum FC.MEM.00389, de 05 de noviembre de 2024, se solicita por la encargada de Ciberseguridad del FOSIS Central, aprobar por acto administrativo, la Política para el uso de controles criptográficos y gestión de claves SSI-A-8.24, versión 15 de octubre de 2024.

6. Que, por las razones previamente expuestas resulta pertinente aprobar la Política antes individualizado a través del presente acto administrativo.

RESUELVO:

APRUÉBESE la Política para el uso de controles criptográficos y gestión de claves del Fondo de Solidaridad e Inversión Social, FOSIS, cuyo texto íntegro es el siguiente:

1. **OBJETIVO**

Establecer normas para el uso de algoritmos de encriptación y servicios de protección de información a utilizar en el FOSIS y para el uso, protección y vida útil de las claves criptográficas durante toda su vida útil en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

2. **ALCANCE**

Debe ser cumplida por todos los usuarios del FOSIS, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios al FOSIS.

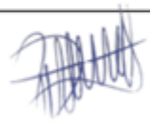
Norma NCH-ISO 27001:2023 controles:

- **A.8.24 Uso de Criptografía**
- **A.5.17 Información de Autenticación**
- **A.5.31 Requisitos legales, estatuarios, reglamentarios y contractuales**

3. **DOCUMENTOS RELACIONADOS**

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, y todos sus procedimientos, políticas, instructivos y circulares.
- NCh-ISO 27001 Of2023 – Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de gestión de la seguridad de la información -Requisitos.
- DS 83/2004, de la Secretaría General de la Presidencia: Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad del documento electrónico.
- Ley 18.834 Estatuto administrativo.
- Ley 18.575 Bases generales de la administración del estado.
- Ley 19.628 sobre protección de la vida privada.
- Ley 19.799 Firma electrónica.
- Ley 19.882 Regula nueva política de personal a funcionarios públicos que indica.
- Ley 19.927 modifica códigos penales en materia de delitos sobre pornografía infantil.
- Ley 20.285 sobre acceso a la información pública.
- DS 93/2006 del Ministerio Secretaría General de la Presidencia, que aprueba norma para minimizar la recepción de mensajes electrónicos no deseados en las casillas de los órganos de la Administración del Estado y de sus funcionarios.
- DS 890/1975 del Ministerio del Interior, fija texto actualizado y refundido de la ley 12.927.

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

Elaborado por: **Roxana Vercoutere Carter** **Encargada Ciberseguridad**	Revisado por: **Gabriel Rosales Villarroel** **Jefe de Tecnologías de la Información y Telecomunicaciones**	Aprobado por: **Cristian Salomó González** **Encargado de Seguridad de la Información** **Subdirector de Usuarios**
		
Fecha: 14/10/2024	Fecha: 16-10-2024	Fecha: 04-11-2024
Documento Impreso – Copia no controlada sin timbre original		

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad de la información	• Apoyar al Comité de Seguridad de la Información en la definición de medidas de protección necesarias. • Validar que las protecciones definidas cumplen con las necesidades institucionales y se encuentren ajustadas a derecho. • Gestionar la resolución de incidencias en el manejo de las cuentas de usuarios.
Jefe de tecnologías de la Información y Telecomunicaciones	• Autorizar formalmente los métodos de encriptación a utilizar en las aplicaciones y sistemas tecnológicos. • Monitorear el cumplimiento de esta política. • Velar por el cumplimiento de las políticas y estándares establecidos para los controles de identificación y autenticación. • Velar por que el desarrollo de las aplicaciones se realice en concordancia con los requisitos descritos en esta política. • Autorizar la asignación de usuarios y contraseñas para personal externo a la institución, cuando corresponda. • Aprobar controles y resguardo de claves de acceso con privilegios.
Jefe del Departamento de Gestión de Personal	• Actuar en forma coordinada con el Departamento de Tecnologías de la Información y Telecomunicaciones, notificando altas, bajas[1].
Fiscal	• Velar por el cumplimiento de la legislación vigente en materias de criptografía y gestión de contraseñas
Comité de Seguridad de la Información	• Aprobar las reglas y estrategias que apoyen la seguridad en el uso de contraseñas y controles criptográficos
Usuarios de FOSIS	• Utilizar sólo algoritmos autorizados por la institución y validados por el jefe de Tecnologías de la Información y Telecomunicaciones. • Cautelar el cumplimiento de las medidas de control del uso de controles criptográficos. • Es responsable de velar por la seguridad de las

ROL	RESPONSABILIDAD
	contraseñas seleccionadas por él mismo para el uso de los distintos servicios y recursos ofrecidos. • Reportar los incidentes de seguridad detectados relacionados con el uso indebido de contraseñas por personas no autorizadas o con el manejo inadecuado de contraseñas. • Reportar violaciones de seguridad en el uso de controles criptográficas como incidentes de seguridad de la información.

5.POLÍTICA

5.1 Generalidades

5.1.1 Declaración institucional

La Seguridad de la Información del FOSIS, es el conjunto de definiciones y acciones destinadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información, a fin de garantizar la continuidad de los procesos de la Institución y mitigar el daño que se les pudiera producir a estos activos.

El uso de contraseña es un aspecto fundamental de la seguridad de los sistemas y recursos informáticos; una contraseña mal elegida o protegida puede generar problemas de seguridad en el FOSIS, específicamente en la protección de la información de la Institución.

El objetivo fundamental de este documento es establecer las reglas para la creación y uso de contraseñas fuertes, favorecer su protección, así como el cambio frecuente de las mismas.

5.1.2 **Definiciones:**

a. Autenticación: Proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático [Decreto N° 83].
b. Contraseña: Una cadena de caracteres protegida, en general encriptada por computador, que autentifica al usuario de un computador en el sistema de información [ISACA 2015].
c. Contraseña predeterminada: La contraseña utilizada para obtener acceso cuando un sistema se instala por primera vez en un computador o dispositivo de red [ISACA 2015].
d. Contraseña robusta: Es la que está diseñada para que sea difícil de descubrir para una persona o un programa. Ya que el propósito de una contraseña es asegurar que solo los usuarios autorizados pueden acceder a los recursos, una contraseña que es fácil de adivinar es un riesgo de seguridad.
e. Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información [ISO 27000:2018].
f. Usuario: Individuo o funcionario que posee una cuenta de usuario de sistemas o servicios de la información del FOSIS.

5.2 **Criptografía**

Se deben definir y aplicar normas para uso eficaz de la criptografía, incluida gestión de claves criptográficas.

Se debe garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos institucionales[2], de seguridad de la información y teniendo en cuenta requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Al utilizar la criptografía, se debe considerar lo siguiente:

a. los principios generales para la protección de la información. Es necesario contar con normas sobre uso de la criptografía para maximizar los beneficios y minimizar los riesgos de uso de las técnicas criptográficas y para evitar un uso inapropiado o incorrecto.
b. identificación de nivel de protección requerido y clasificación de información[3] y, en consecuencia, establecer tipo, fuerza y calidad de algoritmos criptográficos necesarios
c. el uso de criptografía para protección de información contenida en dispositivos finales de los usuarios móviles o en medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento.
d. el enfoque de gestión de claves, incluidos los métodos para tratar la generación y protección de claves criptográficas y recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves;
e. funciones y responsabilidades para:
    - la aplicación de las normas para uso eficaz de criptografía;
    - la gestión de claves, incluyendo la generación de claves (ver procedimiento para la gestión de claves);
f. las normas se adoptan, así como los algoritmos criptográficos, potencia de cifrado, soluciones criptográficas y prácticas de uso que se aprueben o requieran para su utilización en la institución.
g. el impacto de uso de información cifrada en los controles que dependen de la inspección de contenidos (por ejemplo, detección de "malware" o filtrado de contenidos).

La administración adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas.

El sistema de administración de claves se debe basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

a. generación claves para diferentes sistemas criptográficos y diferentes aplicaciones;
b. emisión y obtención de certificados de clave pública;
c. distribución de claves a entidades previstas, incluyendo la forma de activar claves en que se reciben;
d. mantención de claves, incluido el modo en que los usuarios autorizados obtienen acceso a las mismas;
e. cambio o actualización de claves, incluyendo normas sobre en que cambiar claves y cómo se hará;
f. tratamiento de las claves comprometidas;
g. revocación de claves, incluyendo el modo de retirarlas o desactivarlas (por ejemplo, cuando las claves se vieron comprometidas o en que un usuario abandona la institución (en cuyo caso las claves también se deben archivar);
h. recuperación de claves perdidas o dañadas;
i. copia de seguridad o archivo de claves;
j. destrucción de claves;
k. registro y audición de actividades clave relacionadas con gestión;
l. fijación de fechas de activación y desactivación de claves, de modo que estas solo se puedan usar durante el período de tiempo previsto en normas de la institución sobre gestión de claves;
m. gestión de solicitudes legales de acceso a claves criptográficas (por ejemplo, exigir que la información encriptada esté disponible en forma no encriptada como prueba en un caso judicial).

Todas las claves criptográficas deben estar protegidas contra modificación y pérdida. Además, claves secretas y privadas deben estar protegidas contra uso no autorizado y divulgación. Equipo usado para generar, almacenar y archivar claves debe estar protegido físicamente.

Además de la integridad, para muchos casos de uso, también se debe considerar la autenticidad de claves públicas.

La criptografía se usa para alcanzar los siguientes objetivos de seguridad de la información:

5.2.1 **Confidencialidad**

Uso de la encriptación de la información para proteger la información sensible o crítica, ya sea almacenada o transmitida.

Se definen los algoritmos de cifrado que pueden utilizarse al interior del FOSIS, como una aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas.

5.2.2 **Integridad o autenticidad**

Para verificar la autenticidad o integridad de la información almacenada o transmitida sensible o crítica el FOSIS utiliza como mecanismo criptográfico la firma digital bajada en certificados digitales[4].

En el caso de documentos electrónicos, estos son de carácter de firma electrónica avanzada y acorde al cumplimiento de la ley 19.799 con aplicación a los organismos del Estado.

5.2.3 **No repudio**

Uso de técnicas criptográficas para proporcionar evidencia de la ocurrencia o no de un evento o acción.

FOSIS utiliza técnicas de cifrado y firma digital para resolver disputas asociadas al no repudio.

5.2.4 **Autenticación**

Se utilizan técnicas criptográficas para autenticar a los usuarios o entidades externas que requieren hacer uso de los sistemas de información del FOSIS.

Los funcionarios deben usar el sistema autorizado por FOSIS para efecto de autenticación[5].

Si un usuario de FOSIS presenta una denuncia falsa sobre incumplimiento o un comportamiento cuestionable con la intención de perjudicar a otra persona, el denunciante será susceptible de una medida disciplinaria conforme al art. 62 N°9 del DFL 1 del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley 18.575, Orgánica constitucional de bases generales de la administración del estado.

El encargado de seguridad debe ser informado inmediatamente en caso de que se reciba cualquier comunicado por cualquier medio de comunicación de parte de una autoridad de protección de datos u otro ente regulador.

5.3 **Gestión de claves**

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

5.3.1 **Reglas generales**

5.3.1.1Cualquier contraseña es de uso exclusivo e intransferible del usuario al que se ha otorgado.

5.3.1.2 Los usuarios deben cambiar las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio:

Todas las contraseñas de usuarios de sistemas de información o servicios tecnológicos (cuentas de correo, cuentas de servicios web, entre otras) deben cambiarse con la periodicidad establecida en el procedimiento para la gestión de contraseñas vigente.

5.3.2 **Obligaciones de los usuarios**

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas. Las prácticas para aplicar son:

- **Elección de contraseñas**

Los usuarios deben escoger contraseñas robustas o seguras, para todos los sistemas y servicios de información del FOSIS, de la siguiente forma o características:

a. Utilizando al menos doce (12) caracteres, los que deben incluir a lo menos: 1 carácter numérico, una letra del alfabeto mayúscula, una letra del alfabeto minúscula, un carácter especial (por ejemplo: Aam5%$&/).
b. Su longitud depende de la importancia de la información protegida.
c. No ser ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
d. No derivarse del nombre del usuario o de algún pariente cercano.
e. No derivarse de información personal (número de teléfono, cédula de identidad, fecha de nacimiento, entre otros) del usuario o de algún pariente cercano.
f. No se deben usar nuevamente las últimas cinco (5) contraseñas.

- **Uso de contraseñas**

a. Los usuarios no deben compartir de ninguna forma sus cuentas y contraseñas. Estas son estrictamente personales e intransferibles.
b. Los usuarios no deben revelar sus contraseñas por teléfono, correo electrónico, anotándola o de cualquier otra forma a ninguna persona, aun cuando sean jefaturas del FOSIS o administradores de los sistemas.
c. Las contraseñas generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).
d. Ante la sospecha o indicios que una contraseña haya sido comprometida, se debe cambiar la misma de forma inmediata, y se debe a avisar del incidente de seguridad por los cauces establecidos.
e. Un usuario queda bloqueado al cabo de cinco (5) intentos de acceso fallidos. Esta medida protege al sistema frente a ataques de fuerza bruta o de muchos intentos fallidos, lo que se implementa en la medida que sea factible técnicamente.
f. Se deben cambiar las contraseñas en el primer ingreso al sistema o servicio de información.
g. Las contraseñas no deben ser almacenadas en un sistema de registro automatizado (por ejemplo, macros o explorador).
h. Los funcionarios que se conecten a correo electrónico o herramientas de colaboración desde dispositivos móviles tienen la obligación de usar doble factor de autenticación

i. No se deben utilizar las mismas contraseñas personales para fines privados y para fines propio del FOSIS.
j. Si se dispone de diferentes cuentas de acceso a sistemas y servicios de información en el FOSIS, los usuarios deben usar distintas contraseñas para cada una de ellas.
k. Los usuarios nunca deben escribir la contraseña, ni almacenarla en ficheros sin encriptar, ni comunicarla en el texto de mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónico.
l. Todas las contraseñas de administradores (cuentas de administrador, cuentas de administración de aplicaciones, entre otras) deben cambiarse con una periodicidad de al menos una vez cada dos (2) meses.

5.3.3 **Gestión de las contraseñas de usuario**

5.3.3.1 Cuando se asignan y utilizan contraseñas de usuarios, se deben seguir las siguientes reglas:

a. Al firmar los Acuerdos de Confidencialidad, los usuarios también aceptan la obligación de mantener sus contraseñas en forma confidencial, como se establece en este documento.

b. En la medida de lo posible, las contraseñas iniciales deben ser generadas automáticamente con las características recomendadas en la presente política.

c. Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.

d. Cada usuario debe tener la posibilidad de escoger sus propias contraseñas, en los casos que corresponda.

e. Las contraseñas utilizadas para el primer acceso a los sistemas de información deben ser exclusivas y seguras, según lo establecido precedentemente.

f. Las contraseñas de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.

g. Una vez entregadas las credenciales, estas deben estar configuradas con la obligación de cambio posterior al primer inicio de sesión.

h. Todas las credenciales de funcionarios deben tener habilitada su caducidad.

i. El sistema de gestión de contraseñas debe requerir que el usuario cambie obligatoriamente la contraseña de primer acceso cuando ingrese al sistema por primera vez.

j. El sistema de gestión de contraseñas debe requerir que el usuario escoja contraseñas robustas.

k. Si el usuario solicita una nueva contraseña, el sistema de gestión de contraseñas debe determinar la identidad del usuario.

l. Si un usuario ingresa una contraseña incorrecta cinco (5) veces consecutivas, el sistema de gestión de contraseñas debe bloquear la cuenta de usuario en cuestión.

m. Las contraseñas creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.

n. Los archivos que contienen contraseñas deben ser guardados en forma separada de los datos de sistema de la aplicación.

o. No se debe llevar un registro de contraseñas, a menos que un método seguro haya sido aprobado por el Encargado de Seguridad de la Información y estrictamente encriptado.

5.4 Registro y cancelación de registro de usuarios

Este mecanismo de autentificación (claves de acceso, dispositivo u otro) debe ser asignado individualmente, quedando prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.

Toda vez que un funcionario o colaborador que cuente con una cuenta de usuario abandone la organización, el Departamento de Gestión de Personal debe notificar al Departamento de Tecnologías de la Información y Telecomunicaciones a través de Mesa de Ayuda[6] cuando se deba deshabilitar o eliminar su cuenta de usuario de acuerdo con lo establecido en el Procedimiento para término de la relación laboral para planta, contrata y honorarios vigentes.

El Departamento de Gestión de Personas es responsable de notificar por escrito al Departamento de Tecnologías de la Información y Telecomunicaciones sobre el ingreso, salida o traslado de un usuario de acuerdo con lo establecido en los Procedimientos de contratación y movilidad específicamente en el anexo 1 para estos fines. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.

5.5 Asignación de información de autenticación

La administración de los accesos de las cuentas de usuarios se lleva de acuerdo con lo establecido en el procedimiento para la gestión de Administración de contraseñas.

5.6 Contraseña por omisión y recordatorios de contraseña

Toda contraseña por omisión provista por el fabricante de cualquier sistema debe ser reemplazada inmediatamente.

Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos.

Cualquier contraseña encontrada en estos medios debe ser informada al encargado de ciberseguridad a través del registro de gestión de incidentes disponible en intranet[7] y tratada como un incidente.

5.7 Regulación de los controles criptográficos

FOSIS considera los siguientes elementos para el cumplimiento con los acuerdos, las leyes y normativas pertinentes:

a. restricciones sobre la importación o exportación de hardware y software informático para realizar funciones criptográficas;
b. las restricciones sobre la importación o la exportación sobre el hardware y software informático que está diseñado para tener funciones criptográficas agregadas;
c. restricciones sobre el uso del cifrado;

d. métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información cifrada por hardware o software para proporcionar la confidencialidad del contenido.

Todas estas restricciones son monitoreadas por el departamento de Tecnologías de la Información y Telecomunicaciones y reguladas por fiscalía.

6. DIFUSIÓN

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, mediante los siguientes canales:

- Publicación en la intranet del FOSIS
- Correo informativo.

7. SANCIONES

El incumplimiento de las obligaciones emanadas de esta política y todos sus procedimientos asociados será sancionado en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del FOSIS. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. REVISIÓN Y MEDICIÓN

La presente política deberá ser revisada a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

9. CONTROL DE VERSIONES

Versión	Fecha de Aprobación	Motivo del Cambio
1	17/11/2017	Publicación y difusión
2	20/05/2022	Amplía alcance, Agrega punto 5.12, Agrega rol del Fiscal
3	**15/10/2024**	**Actualiza versión de acuerdo con lo establecido en la norma NCh-ISO 27001:2022**

[1] Ver procedimientos de contratación de personal, procedimiento de término de contrato y procedimiento de movilidad

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

vigentes disponibles en intranet
[2] El departamento de informática debe definir e implementar medidas de seguridad, incluidas las normas criptográficas, por varias razones clave: 1. Protección de Datos Sensibles: Las instituciones manejan una gran cantidad de datos sensibles, desde información personal de los clientes hasta propiedad intelectual. Las normas criptográficas ayudan a proteger estos datos contra accesos no autorizados y ciberataques. 2. Integridad de la Información: Es crucial asegurarse de que los datos no sean alterados de manera no autorizada. Las medidas criptográficas verifican la integridad de los datos, asegurando que la información se mantenga precisa y confiable. 3. Confidencialidad: Las normas criptográficas garantizan que solo las personas autorizadas puedan acceder a ciertos datos, protegiendo la confidencialidad de la información sensible. 4. Autenticación y Control de Acceso: La criptografía ayuda en la implementación de métodos de autenticación robustos, asegurando que solo los usuarios autorizados puedan acceder a los sistemas y datos. 5. Cumplimiento Normativo: Muchas industrias están reguladas por leyes que requieren medidas de seguridad específicas. El uso de criptografía adecuada ayuda a las instituciones a cumplir con estas obligaciones legales. 6. Prevención de Fraudes: La implementación de medidas de seguridad criptográficas también ayuda a prevenir fraudes, asegurando que las transacciones y las comunicaciones sean legítimas. 7. Reputación y Confianza: Mantener los datos seguros es vital para la reputación de una organización. Cualquier brecha de seguridad puede dañar la confianza de los usuarios y partes interesadas. Al establecer y mantener estándares criptográficos robustos, el departamento de informática juega un papel crucial en la protección de la infraestructura de tecnología de la información y en la mitigación de riesgos de seguridad. Fuente Estas son consideraciones generalmente aceptadas entre los profesionales del sector, reflejadas en documentos y estándares como los de ISO/IEC 27001 y NIST (National Institute of Standards and Technology)s:
[3] Ver procedimiento para la gestión de activos de información en intranet
[4] Ver FirmaGob
[5] Ver procedimiento para la administración de contraseñas publicado en intranet
[6] Es importante que el aviso sea apenas se materialice la salida del trabajador. No se puede esperar más de 1 día desde el hecho. https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Paginas/Mesa-de-ayuda-Inform%C3%A1tica.aspx
[7] Registro de incidentes de seguridad de la información

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE.

NICOLAS NAVARRETE HERNANDEZ
DIRECTOR EJECUTIVO
FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL

NNH/PMD/FMZ/CSG/RVC/MJCM

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

ANEXOS: SI CORRESPONDE
DISTRIBUCIÓN

- DIRECCIÓN EJECUTIVA (1)
- SUBDIRECCIÓN DE USUARIOS (1)
- SUBDIRECCIÓN DE GESTIÓN DE PROGRAMAS (1)
- SUBDIRECCIÓN DE PERSONAS (1)
- SUBDIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS (1)
- FISCALÍA (1)
- OFICINA DE PARTES (1)
- RESPONSABLE UNIDAD SOLICITANTE: **ROXANA VERCOUTERE CARTER**

Fecha de Emisión: 2024-11-12 (09:40)

Válido indefinidamente

Código Verificación:

DOCUMENTO FIRMADO ELECTRÓNICAMENTE
FOSIS

Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

Documento firmado con FIRMAGOB
Verifique la validez de este documento escaneando el código QR.