	POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES	Fecha emisión: 30/09/2019
	POLÍTICA-SSI-A-10.1.1	Versión: 1
		Fecha versión: 30/09/2019

1. OBJETIVO

Establecer normas para el uso de algoritmos de encriptación y servicios de protección de información a utilizar en FOSIS y para el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.

2. ALCANCE

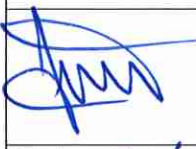


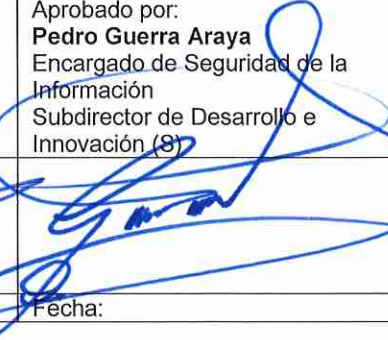
Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes y al uso de algoritmos de cifrado como herramientas de control, protección de la confidencialidad, autenticidad o integridad de la información, así como la debida documentación y resguardo de estos.

Norma NCH-ISO 27001:2013 controles:

- A.10.1.1 Política sobre uso de controles criptográficos
- A.10.1.2 Gestión de claves
- A.09.3.1 Uso de información confidencial para la autenticación

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, Res. 0879/12-07-2019.
- NCh-ISO 27001:2013 – Tecnología de la información -Técnicas de seguridad – Sistema 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 19.223 sobre figuras penales relativas a la informática.
- Ley 19.628 sobre protección de la vida privada.
- Ley 19.799 Firma electrónica.
- Ley 19.927 modifica códigos penales en materia de delitos sobre pornografía infantil.
- Ley 20.285 sobre acceso a la información pública.

Elaborado por: Armando Guajardo San Martín Roxana Vercoutere Carter Profesionales Depto. Procesos y Mejora Continua	Revisado por: Gabriel Rosales Villarroel Jefe Departamento de Soporte y Operaciones TIC	Aprobado por: Pedro Guerra Araya Encargado de Seguridad de la Información Subdirector de Desarrollo e Innovación (S)
 		
Fecha: 30/09/2019	Fecha: 30/09/2019	Fecha:
Documento Impreso – Copia no controlada sin timbre original		

POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES

- DS 81/2004 del Ministerio Secretaría General de la Presidencia, aprueba Norma técnica para los órganos de Administración del Estado sobre interoperabilidad de documentos electrónicos.
- 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 100/2006 del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para el desarrollo de sitios web de los órganos de la Administración del Estado.
- DS 890/1975 del Ministerio del Interior, fija texto actualizado y refundido de la ley 12.927.
- Política de control de acceso FOSIS.

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad de la información	<p>Apoyar al comité de seguridad de la información en la definición de medidas de protección necesarias.</p> <p>Validar que las protecciones definidas cumplen con las necesidades institucionales y se encuentren ajustadas a derecho.</p> <p>Gestionar la resolución de incidencias en el manejo de las cuentas de usuarios.</p>
Jefe Departamento de transformación digital	<p>Verificar que en el desarrollo de nuevos sistemas o modificaciones de estos se empleen sólo los algoritmos autorizados por el FOSIS.</p>
Jefe Departamento de soporte y operaciones TIC	<p>Instruir formalmente los métodos de encriptación a utilizar en las aplicaciones y sistemas tecnológicos.</p> <p>Generar e implementar los controles definidos en los procesos que afectan el control de uso de controles criptográficos.</p> <p>Administrar claves criptográficas.</p> <p>Identificar las áreas de acuerdo con la tipificación de seguridad del control de uso de controles criptográficos.</p> <p>Definir los controles necesarios para el control del uso de controles criptográficos.</p> <p>Monitorear el cumplimiento de esta política.</p> <p>Definir controles para el resguardo de claves de acceso.</p> <p>Velar por el cumplimiento de las políticas y estándares establecidos para los controles de identificación y autenticación.</p> <p>Gestionar los accesos de usuarios a las aplicaciones, resguardar las contraseñas de administración.</p> <p>Velar porque el desarrollo de las aplicaciones se realice en concordancia con los requisitos descritos en esta política.</p> <p>Autorizar la asignación de usuarios y contraseñas para personal externo a la institución.</p> <p>Aprobar controles y resguardo de claves de acceso con privilegios.</p>

POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES

ROL	RESPONSABILIDAD
Jefe del Departamento de gestión de personal	Actuar en forma coordinada con el Departamento de Soporte y Operaciones TIC, notificando altas y bajas.
Funcionarios de planta, contrata, honorarios y prestadores de servicios	Cautelar el cumplimiento de las medidas de control del uso de controles criptográficos. Cada miembro del personal FOSIS debe tener asignada una cuenta de usuario segura (con su correspondiente usuario y contraseña), para acceder a los recursos y activos de información de la red informática institucional, y asumirá la responsabilidad de la correcta utilización y mantenimiento de esta credencial, teniendo presente que los datos de su cuenta de usuario son personales e individuales. Reportar supuestas violaciones de seguridad en el uso de controles y claves criptográficas como incidentes de seguridad de la información.

5. POLÍTICA

5.1 Generalidades

Se debe cifrar toda la información sensible, clasificada como de riesgo alto, que pudiese quedar expuesta a usuarios no autorizados, con relación a su privacidad e integridad.

Se deben utilizar controles criptográficos para la protección de la confidencialidad, el cumplimiento del principio de la no repudiación y el control de integridad de la información en los siguientes casos:

- Protección de claves de acceso a sistemas, documento electrónico, datos y servicios.
- Transmisión de información clasificada fuera del ámbito del servicio.
- Resguardo de información cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el encargado de seguridad de la información.

5.2 Acerca de la confidencialidad

Se definen los algoritmos de cifrado que podrán 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.

Sólo se utilizan algoritmos de cifrado definidos en estándares internacionales.

5.3 Acerca de la integridad/autenticidad

Para verificar la autenticidad o integridad de la información almacenada o transmitida sensible o crítica, el FOSIS podrá utilizar como mecanismo criptográfico la firma digital bajada en certificados digitales.

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.

POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES

5.4 Acerca del no repudio

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

5.5 Acerca de la 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.

El encargado de seguridad debe ser informado por el jefe del Departamento de soporte y operaciones TIC 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, siguiendo las pautas establecidas en el procedimiento para el contacto con las autoridades (PR – SSI- 06.01.03 Procedimiento para el contacto con las autoridades y grupos de interés.)

5.5 Registro y cancelación de registro de usuarios

Este mecanismo de autenticación (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 deberá notificar al Departamento de soporte y operaciones TIC cuando se deba deshabilitar o eliminar su cuenta de usuario de acuerdo a lo establecido en los PR GDP-6.2.1-09 Procedimiento para término de la relación laboral para planta y contrata y PRGDP-6.2.1-10 Procedimiento término de la relación laboral para el personal a honorarios.

El Departamento de Gestión de Personas es responsable de notificar por escrito al Departamento de soporte y operaciones TIC sobre el ingreso, salida o traslado de un usuario de acuerdo a 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.

5.6 Administración de la información de autenticación secreta de los usuarios (usuario y contraseña)

La administración de los accesos de las cuentas de usuarios se llevará de acuerdo a lo establecido en el procedimiento de gestión de Administración de contraseñas (PR-SDI 9.4.3-01).

5.7 Uso de la información de autenticación secreta

Todos los funcionarios, personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el FOSIS tienen la obligación de cumplir con las siguientes directrices:

POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES

- Mantener la información de autenticación secreta como confidencial, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad.
- Evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.
- Cambiar la información de autenticación secreta cuando exista alguna sospecha de que pudiera haber sido vulnerada o conocida por terceros.
- No se debe compartir la información de autenticación secreta de usuario de una persona.
- No se debe utilizar la misma información de autenticación secreta para fines distintos a los relacionados con las actividades de FOSIS (por ejemplo: cuentas personales de redes sociales, bancos, casas comerciales, etc.)

5.8 Contraseñas en Dispositivos de Red

Todos los dispositivos de red (routers, firewalls, switches) deben tener contraseñas únicas u otro mecanismo de control de acceso.

Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

5.9 Contraseña por Omisión

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

5.10 Recordatorios de Contraseñas

Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos. Cualquier contraseña encontrada en estos medios será informada al encargado de seguridad y tratada como un incidente.

5.11 Acceso a Información Sensible

En el caso del control de acceso a información, se deben utilizar contraseñas robustas seguras o cifradas.

La contraseña nunca debe ser compartida o relevada; hacer esto responsabiliza al usuario que prestó la contraseña de acceso y a todas las acciones que se realicen de la misma. Frente a la evidencia de un compromiso del sistema por uso indebido de cuentas con privilegios, todas las contraseñas de cuentas con privilegios del sistema deberán ser reemplazadas.

Los usuarios o administradores de FOSIS deberán informar cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los sistemas a sus superiores, al Departamento de soporte y operaciones TIC y al Encargado de Seguridad.

POLÍTICA PARA EL USO DE CONTROLES CRIPTOGRAFICOS Y GESTIÓN DE CLAVES

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 de 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 tres 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	30/09/2019	Publicación y difusión