POLÍTICA DE CONTROLES CRIPTOGRÁFICOS STECSDI

Elaborado Por:				
Fecha	**Nombre**	**Cargo**	**Versión**	**Firma**
26/04/2023	Diego Moreira	Asistente de Tecnologías de la Información y Comunicación 1	1.0	Firmado electrónicamente por: DIEGO ANDRE MOREIRA ALDEAN

Revisado Por:				
Fecha	**Nombre**	**Cargo**	**Versión**	**Firma**
26/04/2023	José Luis Alcarraz	Analista de Tecnologías de la Información y Comunicación 1	1.0	Firmado electrónicamente por: JOSE LUIS ALCARRAZ ROMERO

Aprobado Por:				
Fecha	**Nombre**	**Cargo**	**Versión**	**Firma**
26/04/2023	Ronald Sarmiento	Director Administrativo	1.0	Firmado electrónicamente por: RONALD GABRIEL SARMIENTO MARTINEZ

Control de Cambios

Versión	Fecha	Descripción del cambio	Elaborado por:	Solicitado por:
1.0	26/04/2023	Elaboración de la primera versión de la política de controles criptográficos STECSDI	UGT	CSI
2.0				
3.0				

Cláusula de Confidencialidad

Contenido

1.- Antecedentes

Con fecha 20 de septiembre del 2019, El Ministerio de Telecomunicaciones y de la Sociedad de la Información a través del Acuerdo Ministerial No.025-2019 expidió el Esquema Gubernamental de Seguridad de la Información - EGSI (versión 2.0), el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva (APC).

Con fecha 28 de junio del 2022, mediante oficio Nro. STECSDI-STECSDI-2022-0173-OF la máxima autoridad de la Secretaria Técnica Ecuador Crece Sin Desnutrición infantil designa al analista de tecnología José Luis Alcarraz Romero como nuevo oficial de seguridad de la información.

Con fecha 8 de julio del 2022, mediante memorando STECSDI-SGIIE-2022-0124-M se comunica al Comité de Seguridad de la Información lo siguiente:

“Conforme a lo resuelto en el segundo punto del orden del día de la II Sesión Ordinaria del Comité de Seguridad de la Información (CSI) de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil, llevada a cabo el día 21 de junio de 2022 a las 15h00, el señor Ingeniero José Luis Alcarraz Romero - Analista de Tecnología de la Información y Comunicaciones 1 ha sido designado como Oficial de Seguridad de la Información (OSI) de la Secretaría Técnica Ecuador Crece sin Desnutrición Infantil.”

2.- Objetivo

Garantizar un correcto y eficaz uso de la criptografía para asegurar la confidencialidad, autenticidad e integridad de la información digital de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil.

3.- Ámbito de Aplicación

Esta política aplica para toda la información digital que genere la Secretaria Técnica Ecuador Crece Sin Desnutrición Infantil que, en función de su clasificación, naturaleza o por pedido explícito requiera ser protegida de esta forma, para mantener la confidencialidad, autenticidad e integridad de la misma.

La Política de controles criptográficos es aplicable a todo el personal de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil tanto para el personal en planta central, así como también al personal que se encuentran en las 8 zonas del territorio nacional.

Los proveedores de la STECSDI tanto del sector privado como el público que ofrezcan o proporcionen sistemas, software o aplicaciones móviles a la Secretaria Técnica Ecuador Crece Sin Desnutrición Infantil.

4.- Marco Jurídico

Guía para la implementación de controles de seguridad de la información (NTEINEN ISO/IEC 27002:2017) perteneciente al Esquema Gubernamental de Seguridad de la Información EGSI V2, emitido en Acuerdo Ministerial No. 25 - 2019 con Registro Oficial Edición Especial 228 de 10 - ene - 2020.

El esquema de seguridad de la información en cuanto al uso de controles criptográficos establece lo siguiente:

Sección 6 Criptografía

6.1.1 Política de uso de los controles criptográficos
6.1.2 Gestión de claves

Sección 14 Cumplimiento

14.1.5 Reglamento de controles criptográficos

5.- Política de controles criptográficos.

5.1 Entrega credenciales

Todas las credenciales de acceso (usuario y contraseña) para todas las aplicaciones o sistemas institucionales entregadas o generadas por los funcionarios de la STECSDI, deberán contar con el respectivo cifrado el cual puede ser el que se proporcione por el proveedor de la aplicación o sistema, desarrollado por la Dirección de Seguimiento Nominal o implementado por la unidad de tecnología de la STECSDI.

5.2 Cambio de contraseña

Comunicar por medio de la mesa de ayuda de tecnología (soporte.tecnologia@infancia.gob.ec) para solicitar el cambio de contraseña de la sesión ya sea la contraseña de usuario Windows, contraseña de correo electrónico, contraseña de Quipux o contraseña de VPN, es importante mencionar que la contraseña para acceso a las carpetas compartidas de las diferentes direcciones es la misma contraseña de usuario de Windows que se las administra por medio del directorio activo de la institución.

5.3 Bloqueo de usuarios

Posterior a cinco intentos fallidos de autenticación de usuario el sistema bloqueará por diez minutos al usuario involucrado, para el desbloqueo de los usuarios se deberá enviar un requerimiento del olvido de contraseña a través de la mesa de ayuda de tecnología.

5.4 Eliminación usuarios y privilegios

En los casos en que un funcionario o colaborador que le haya sido entregada con una cuenta de usuario y este abandone la institución, la Dirección de Talento Humano debe notificar a la Unidad de Tecnología a través de un correo a la mesa de servicio cuando se deba deshabilitar o eliminar su cuenta de usuario, de igual manera en los casos de rotación de personal entre direcciones la dirección de talento humano deberá notificar a la unidad de tecnología para proceder con la inhabilitación, modificación o eliminación de acceso y privilegios.

5.5 Cifrado de respaldos

Los respaldos automáticos de todas las carpetas compartidas de la STECSDI tanto full backups como respaldos incrementales semanales cuentan con cifrado proporcionado por la aplicación Duplicati versión 2 canary, el cifrado implementado actualmente para la protección estas carpetas es AES-256.

5.6 VPN IPSEC

Dado que nuestra institución no cuenta con acceso a la red nacional gubernamental las conexiones punto a punto con otras instituciones del sector público se las realiza mediante la implementación de VPN IPSEC en el cuales se implementa el cifrado AES_CBC_256 en unos casos y el cifrado 3DES-CBC.

5.7 VPN SSL/TSL

Para acceso a las carpetas compartidas y aplicaciones que se encuentran en planta central se proporciona a los funcionarios el uso de una vpn ssl administradas a través del firewall pfsense versión 2.6.0 el cual implementa un cifrado AES-256-GCM.

En cuanto al acceso remoto al entorno de producción (Sistemas Seguimiento Nominal) estas vpns se manejan a través del firewall Sophos UTM 9 el cual proporciona un cifrado AES-128-CBC.

6.- Glosario

Advanced Encryption Standard (AES): también conocido como Rijndael (pronunciado "Rain Dahl" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos, creado en Bélgica.

Contraseña: Código secreto compuesto por una cadena de caracteres que pueden ser especiales y alfanuméricos, que se introduce en un sistema, equipo informático o red para iniciarlo y acceder para operarlo.

Controles criptográficos: Formas de codificar información para que no pueda ser alterada, interpretada o dañada, para posteriormente decodificarla y que se presente íntegra y tal cual es.

Credenciales de acceso: Son el nombre de usuario y contraseña gestionados que dan acceso a un sistema o equipo.

Criptografía: Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Ipsec: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

SSL: es un protocolo criptográfico, que proporcionan comunicaciones seguras por una red, comúnmente Internet.

VPN: (*virtual private network*,) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos