Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil

Política de Seguridad de la Información.

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Versión. 2.0

Agosto 2022

Firmas de Responsabilidad

		NOMBRE	CARGO	FECHA	FIRMA
APROBADO POR	COMITÉ DE SEGURIDA DE LA INFORMACIÓN	Juan Carlos Palacios	**Presidente del Comité de Seguridad de la Información**	Agosto 2022	Firmado electrónicamente por: **JUAN CARLOS PALACIOS MORA**
REVISADO POR:	OFICIAL DE SEGURIDA DE LA INFORMACIÓN	José Luis Alcarraz	Oficial de Seguridad de la Información	Agosto 2022	Firmado electrónicamente por: **JOSE LUIS ALCARRAZ ROMERO**
ELABORADO POR:	Técnico	Erick Andrade	Analista de Tecnología de la Información y Comunicación 3	Agosto 2022	Firmado electrónicamente por: **ERICK PAUL ANDRADE SANTAMARIA**

Control de Cambios

Versión	Fecha	Descripción del cambio	Elaborado por:	Solicitado por:
1.0		-	-	-
2.0	08/08/2022	Actualización	Erick Andráde	José Luis Alcarraz

Tabla de contenido

1. INTRODUCCIÓN

El Esquema Gubernamental de Seguridad de la Información EGSI versión 2.0, emitido mediante Acuerdo Ministerial No. 025-2019, y publicado en el Registro oficial Nro. 228 del 10 de enero del 2020.

Art. 1.- Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependes de la Función Ejecutiva.

Art. 3.- Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependes de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información

Art. 4.- Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial.

EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI señala:

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1.1 Políticas de la Seguridad de la Información

Control

Elaborar, implementar y socializar las políticas de seguridad de la información, definidas para la institución, debidamente aprobada por la Máxima Autoridad o su delegado.

Recomendaciones para la implementación:

1.1.1.1 La máxima autoridad dispondrá la implementación de este Esquema Gubernamental de seguridad de la Información en su institución

En virtud de lo expuesto, y, en función de las competencias y atribuciones de la Unidad de Tecnología de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil, se elabora la actualización del documento "Política de Seguridad de la Información", a fin de ponerlo a consideración del Comité de Seguridad de la Información para su análisis y posterior aprobación por parte de la máxima autoridad o su delegado.

2. ANTECEDENTES

La Política de Seguridad de Información, establece el marco de referencia a través del cual la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil (STECSDI) implementará el Sistema de Gestión de Seguridad de Información (SGSI) de la Secretaría, fijando así los estándares de

seguridad de la información a aplicar para administrar adecuadamente sus activos de información. De conformidad a lo establecido en el Acuerdo Ministerial No. 025-2019, y publicado en el Registro oficial Nro. 228 del 10 de enero del 2020 y las normas ISO 27000, se consideran los siguientes elementos centrales:

- La disponibilidad, integridad y confidencialidad de la información.
- La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
- El levantamiento y categorización de los activos de información, y sus responsables.
- La gestión de riesgos que afecten a los activos de información, frente a amenazas internas o externas, deliberadas o accidentales.
- La operación correcta y segura de las instalaciones de procesamiento de información.
- La seguridad física y del entorno donde se encuentran y operan los activos de información.
- La relación con los proveedores y usuarios externos.
- La legislación vigente en lo referente a la definición de la información pública, confidencial y reservada.

3. CONSIDERACIONES GENERALES

3.1. Declaración de la Política de Seguridad de la Información

La STECSDI se compromete a desarrollar los procesos de Gestión de Seguridad de la Información cumpliendo con los principios de confidencialidad, integridad y disponibilidad de los activos de información, promoviendo una gestión eficaz de riesgos y generando una cultura de seguridad, que contribuya al logro de los objetivos institucionales en base al Esquema Gubernamental de Seguridad de la Información EGSI versión 2.0, emitido mediante Acuerdo Ministerial No. 025-2019, y publicado en el Registro oficial Nro. 228 del 10 de enero del 2020.

3.2. Descripción General de la Política

Incorporar políticas, normas y procedimientos para la seguridad de la información, y la aplicación de estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información. Por ello, es necesario que se cumplan las normativas que se dicten y estén vigentes a través de la implantación de un proceso de Seguridad de la Información único, orientado al resguardo de los activos de información.

Las directrices y alcances contenidos en este documento son susceptibles de mejora continua, por lo tanto, son factibles de modificaciones, actualizaciones y cambios periódicos, tendientes a mantenerlas vigentes y aplicables de acuerdo con las condiciones que la STECSDI requiera.

3.3. Objetivos de la Política Interna

- Asegurar el cumplimiento de la política de seguridad de la información y que sus objetivos sean compatibles.
- Asegurar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la STECSDI.
- Asegurar que el proceso de gestión de seguridad de la información alcance los resultados previstos.
- Identificar, clasificar, categorizar y mantener actualizados los activos de información.
- Identificar a los responsables de la administración y custodia de los activos de información.
- Determinar los roles, responsabilidades y competencias de los funcionarios que tengan relación con la gestión de seguridad de la información.
- Asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento.
- Detectar, eliminar o mitigar los riesgos que amenacen los activos de información.
- Establecer, actualizar y difundir las normas, procedimientos e instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- Mantener actualizado y monitorear el proceso de Gestión de Seguridad de la Información y establecer los mecanismos de seguimiento y control de los activos de información y tecnologías de procesamiento.
- Difundir la Política de Seguridad de la Información y capacitar a todos los funcionarios de la STECSDI.

3.4. Roles y Responsabilidades

Para cumplir con los objetivos de la Política de Seguridad de la Información de la STECSDI se establecen los siguientes roles y responsabilidades:

La/El Secretario /a Técnico/a (Máxima autoridad o su delegado/a)

- Responsable de revisar, aprobar y suscribir en general todos los documentos relacionados con las políticas de seguridad de la información.

El comité de Seguridad de la Información tendrá como principales responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

e) Promover la difusión de la seguridad de la información dentro de la institución.
f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
g) El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.
h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema.

Oficial de Seguridad de la Información

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI),
e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.
f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
h) Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.
i) Mantener la documentación de la implementación del EGSI debidamente organizada.
j) Verificar el cumplimiento de las norman procedimientos y controles de seguridad institucionales establecidos.
k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.
l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

Funcionarios (as) de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil

Son los servidores públicos que administran los activos de información, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente y además tienen la obligación de reportar los eventos que ponen en riesgo la seguridad de la información.

4. POLÍTICAS INTERNAS

4.1. Generales

- Todos los funcionarios de la STECSDI deberán observar y cumplir lo estipulado en el presente documento en coordinación con el oficial de seguridad de la información
- Todos los funcionarios que se vinculen a la Institución sin excepción deberán firmar el acuerdo de confidencialidad, el mismo que será parte del expediente y estará almacenado en el archivo de Talento Humano.
- El desconocimiento del contenido de este documento no lo exonera de las responsabilidades asociadas con su incumplimiento y de las sanciones que establecerán las autoridades institucionales.
- Toda información generada, modificada o procesada en la institución es de propiedad exclusiva de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil.
- Todo funcionario respetará la naturaleza confidencial de datos o cualquier otra información que pueda caer en su poder, sea como parte de su trabajo o por accidente.
- El personal de la unidad de Tecnologías de la Información y Comunicación, respetará la privacidad de los usuarios, no divulgará información acerca de las cuentas de usuario o del uso que haga del servicio a menos que sea requerido por escrito por la máxima autoridad para cumplir con procedimientos legales.
- Los usuarios tendrán derecho a la confidencialidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de los datos institucionales, así como para responder ante quejas sobre contenidos que violen los derechos de terceras personas.
- En los casos que se detecten acciones que puedan poner en riesgo la seguridad o los niveles de eficiencia, tanto de la red de datos e información institucional como de cualquiera de los componentes de la misma, el responsable de la UGT podrá realizar una auditoría y emitir recomendaciones para prevenir o corregir estas situaciones.
- Los funcionarios de la STECSDI deberán respetar de manera obligatoria, las políticas de seguridad propias de cada una de las instituciones que proporcionan acceso a sus sistemas como Quipux, Esigef, SIPEIP, SERCOP, SRI, IESS, etc.

- Se prohíbe acceder a través de la red a los sistemas de información, servicios y bases de datos de la Institución, para los cuales no se le ha otorgado el permiso.
- Se prohíbe modificar o eliminar la información almacenada en el computador asignado, cuando el funcionario sea transferido de la Unidad y/o retirado de la Institución.
- Los funcionarios que realicen algún intento o acción sobre los recursos que ponga en riesgo la integridad, disponibilidad, eficacia, eficiencia, confidencialidad y/o fiabilidad de la información, el oficial de seguridad reportará a la Unidad Administrativa de Talento Humano con el fin de que proceda con las sanciones correspondientes de acuerdo a lo señalado en la normativa vigente.

4.2. De la Seguridad de la Información

4.2.1 DE LAS CONTRASEÑAS

De los funcionarios de la STECSDI

- Las cuentas de usuario y las contraseñas de acceso a los sistemas tanto internos como externos son personales e intransferibles y son de uso único de los funcionarios de la institución.
- Serán responsables de resguardar y proteger las claves de acceso asignadas por las unidades competentes (usuario y contraseña) para evitar accesos no autorizados.
- Para la generación de claves deberán incorporar letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta.

De la Gestión de Tecnología.

- Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros.
- Definir que la construcción de contraseñas para los usuarios tenga al menos 8 caracteres alfanuméricos, incluyendo adicionalmente caracteres especiales.
- Establecer la caducidad de las contraseñas en un período no superior a 60 días.
- Forzar el uso de credenciales de autenticación únicas.
- Evitar contraseñas en blanco o que viene por defecto según el sistema o el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros.

4.2.2 DEL SERVICIO DE CORREO ELECTRÓNICO

De los funcionarios de la STECSDI

- La dirección de correo electrónico con el dominio @infancia.gob.ec, será utilizado única y exclusivamente para temas institucionales.
- Cada funcionario es responsable tanto del contenido del mensaje enviado como de sus adjuntos.
- Los funcionarios deberán respaldar su buzón de correo electrónico y almacenarán en un lugar seguro al menos 3 veces al año.
- Está prohibido el uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros para temas institucionales.
- Los funcionarios deberán eliminar inmediatamente los mensajes con origen desconocido y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos.
- Los funcionarios son los responsables de la cantidad y tamaño de mensajes que envíe, evitando generar spam a través del envío de correo masivo, el máximo número de destinatarios por correo máximo 30.
- Los funcionarios que necesiten la creación y uso de cuentas de correo diferentes a la asiganada para uso institucional deberá llenar el formulario de cuenta adcional de correo anexo 4, el mismo debe estar firmado por el funcionario solicitante y su jefe inmediato.

De la Gestión de Tecnología.

- Realizará monitoreo de los mensajes.
- Mantener el respaldo del buzón de correo de los funcionarios cesantes en los plazos establecido por la normativa.
- Asignar una única cuenta de correo electrónico a cada funcionario de la STECSDI, asociada con la primera letra de su nombre y apellido.
- El límite de espacio máximo de cada buzón de correo signado al jerárquico superior es de 10GB, para el resto de funcionarios se asignará un tamaño máximo de 4GB.
- Asegurar que el antivirus instalado en la institución monitoree los mensajes de correo y los adjuntos antes de su ejecución.
- Verificar que la plataforma utilizada para el funcionamiento del correo electrónico contenga el cifrado de datos.

- Controlará el envío no autorizado de correo masivo en coordinación con el proveedor del servicio.
- Capacitará a los funcionarios de la Institución sobre el uso adecuado del correo electrónico y el proceso para la obtención de los respaldos de su buzón.

4.2.3 DEL SERVICIO DE INTERNET.

De los funcionarios de la STECSDI

- Este servicio debe utilizarse exclusivamente para las tareas propias de la función asignada por la institución, no debe utilizarse para ningún otro fin.
- Cada usuario es responsable de la información y contenidos a los que accede y de aquella información que copia para conservación en los equipos de la institución.
- Los funcionarios que por la naturaleza de sus funciones requieran acceso a redes sociales, youtube, whatsapp web, o a algún sitio determinado como restringido, deberá llenar el formulario "ACCESO A SITIOS WEB RESTRINGIDOS" señalado en el **Anexo 1**, el mismo que deberá estar autorizado por el director de la Unidad Administrativa correspondiente.

De la Gestión de Tecnología.

- Limitar a los usuarios el acceso a portales, aplicaciones o servicios de Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, bloqueará el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución y particularmente a los que atenten a la ética y moral.
- Monitorear los accesos de los funcionarios a las diferentes aplicaciones y contenidos.
- Bloquear o limitar el acceso y uso de Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.
- No puede contratar el acceso y uso de servicios de correo electrónico en Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio

nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

4.2.4 DE LOS RESPALDOS DE INFORMACIÓN

De los funcionarios de la STECSDI

- Realizar de manera periódica su propio respaldo de la información institucional generada, tales como: Carpetas compartidas, buzón de correo y cualquier carpeta local que el funcionario creyere conveniente, y almacenarla en algún medio físico DVD, pen drive, disco externo, etc.
- Almacenar la información crítica de su gestión en las carpetas compartidas asignadas a cada unidad administrativa, la información guardada en carpetas diferentes a las señaladas, no se respaldarán.
-

De la Gestión de Tecnología.

- La unidad de tecnología, tiene la tarea de establecer y ejecutar un mecanismo para el resguardo de la información contenida en las carpetas compartidas y la información del centro de datos de la STECSDI.
- Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres generados en la institución.
- Capacitará a los funcionarios de la Institución sobre la manera adecuada de generar sus propios respaldos sea esto del correo electrónico, Quipux, carpeta local y carpetas compartidas.

4.2.5 DE LAS CARPETAS COMPARTIDAS

De los funcionarios

- Los funcionarios almacenarán información en las carpetas compartidas única y exclusivamente datos institucionales.

- Las carpetas compartidas se han creado una por cada unidad administrativa, por lo tanto, no están autorizados a eliminar información que no les pertenece.
- Los funcionarios solicitarán acceso a las carpetas compartidas de su unidad administrativa a través del formulario "CREACIÓN /ACCESO A CARPETAS COMPARTIDAS", **Anexo 2**, el mismo que deberá estar debidamente justificado y autorizado por el director del área correspondiente.
- Los funcionarios deben mantener depuradas las carpetas compartidas asignadas para su uso.

De la Gestión de Tecnología.

- Creará una carpeta en el servidor de respaldo o disco NAS, la misma que será compartida a cada una de las unidades administrativas de la Institución, para el almacenamiento de la información Institucional.
- En el escritorio de cada uno de los computadores de los funcionarios creará un acceso directo hacia la carpeta compartida asignada para su uso.
-

4.2.6 DEL HARWARE

De los funcionarios de la STECSDI

- Tienen la obligación de mantener en óptimas condiciones los computadores de escritorio, laptops, impresoras y de más equipos que la STECSDI ha asignado como herramientas de trabajo.
- En caso de presentar algún desperfecto en los equipos debe notificar de manera inmediata al personal técnico de la Unidad de tecnología y a la dirección administrativa.
- Si por razones institucionales existe la necesidad de sacar su computador fuera de la institución deberá coordinar con el responsable de bienes la autorización respectiva.
-

De la Gestión de Tecnología.

- El data center de la institución es un área restringida, no se permitirá el ingreso de funcionarios sin autorización.

- Tiene la responsabilidad de verificar que el o los equipos asignados a los funcionarios estén funcionando de manera correcta, reportará su estado a la dirección administrativa a través de un informe técnico.
- Elaborar el Plan de mantenimiento preventivo y correctivo.
- La unidad de tecnologías es la responsable del mantenimiento preventivo y correctivo del hardware de la institución, que lo realizará de manera periódica al menos 2 veces al año.
- La unidad de tecnología realizará el monitoreo y garantiza el correcto funcionamiento de: Equipos de comunicación, firewall, servidores, aire acondicionado, etc., equipos almacenado en el data center institucional.

4.2.7 DEL SOFTWARE

De los funcionarios

- Todos los funcionarios de la institución están prohibidos instalar programas o software no autorizado por la Institución.
- Todos los funcionarios de la institución están prohibidos borrar cualquiera de los programas instalados por la unidad de tics es los equipos asignados para su uso.
- Verificará antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.
- Previo al desarrollo de software con personal institucional, a la formulación de términos de referencia o especificaciones técnicas para el desarrollo o adquisición de una solución de software deberá solicitar a la Unidad de Tecnología la certificación de existencia del software sea este similar o equivalente, catálogo publicado en www.softwarepublico.gob.ec.

De la Gestión de Tecnología.

- Antes de que el equipo se entregue a los nuevos funcionarios deberá verificar que estén instalados todos los programas necesarios para el desarrollo de sus actividades diarias.
- Monitorear, instalar y actualizar de manera periódica el software antivirus en los computadores de la STECSDI.
- Mantener actualizadas a las últimas versiones de seguridad, los sistemas operativos y sistemas de procesamiento de información.
- Revisar periódicamente el contenido de software y datos en los equipos que sustentan procesos críticos de la institución.

- Emitir boletines informativos de alerta con información precisa.
- Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.
- Dar cumplimiento al Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública.
- Previo al desarrollo de software con personal institucional, emitirá una certificación de existencia del software sea este similar o equivalente, del catálogo publicado en www.softwarepublico.gob.ec, a fin de dar estricto cumplimiento al Oficio Nro. PR-SGPR-2019-3927-O, emitido por el Secretario General de la Presidencia de la República el 25 de Octubre de 2019.

4.2.8 DE LAS VIDEOCONFERENCIAS

De los funcionarios

- Solicitar salas virtuales para videoconferencias al correo soporte.tecnologia@infancia.gob.ec, señalando el día, la hora, asunto, lista de asistentes
- Está prohibido compartir el link de la sala virtual a persona no convocadas, no autorizadas o ajenas a la Institución.
- Deberán ingresar a la videoconferencia con el micrófono y cámara apagados al menos 10 minutos de la hora convocada.
- Deberán ingresar a las videoconferencias señalando el nombre y apellido del funcionario de la STECSDI, está prohibido utilizar seudónimos o nombres de familiares.
- El organizador de la videoconferencia verificará que únicamente participen personas autorizadas.
- Está prohibido conectarse a las video conferencias desde lugares públicos.
- Está prohibido las grabaciones de audio y video, sin la autorización expresa del organizador, autor o la persona que tenga los derechos sobre el material.

De la Gestión de Tecnología.

- Gestionar la adquisición la licencia de un software para videoconferencias acorde a las necesidades institucionales.
- Definir un responsable para administrar las videoconferencias.

- Remitir el link de acceso a la videoconferencia a todos los participantes.
- Iniciar las salas virtuales.
- Verificar que los dispositivos micrófono y parlantes funcionen de manera correcta en los computadores de los funcionarios de la STECSDI.
- Monitorear eventualmente las videoconferencias para verificar el cumplimiento de la política de seguridad.

4.2.9 DE LA GESTIÓN DE LA INFORMACIÓN CON TERCEROS

Previo a la entrega de bases de datos de información confidencial generada en la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil, se debe realizar la suscripción del Acuerdo de Confidencialidad (**Anexo 3**) entre el peticionario de la información y el dueño del proceso de la STECSDI.

Información Confidencial: Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones al derecho de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

Información pública: Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere la LOTAIP y contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

5. SANCIONES

Se regirá conforme a lo establecido en el Reglamento General a la Ley Orgánica del
Servicio Público.

6. GLOSARIO DE TÉRMINOS

Activos de Información: Comprende a los sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información.

Ataque: Intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

CSI: Comité de seguridad de la información.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Incidente: Es un suceso repentino no deseado que ocurre por las mismas causas que se presentan los accidentes, sólo que por cuestiones del azar no desencadena lesiones en las personas, daños a la propiedad, al proceso o al ambiente. Un incidente es una alerta que es necesario atender.

Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

EGSI: Esquema gubernamental de Seguridad de la Información

Norma ISO: Norma definida por la Organización Internacional de Normalización que se aplica a los productos y servicios.

Seguridad de los Activos de Información: Asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la STECSDI.

Seguridad de la Información: Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad

7. ANEXOS

Gobierno del Encuentro

GUILLERMO LASSO
PRESIDENTE

UNIDAD DE GESTIÓN DE TECNOLOGÍAS FORMULARIO ACCESO A SITIOS WEB RESTRINGIDOS

DATOS DEL FORMULARIO

Fecha: **No.** UGT-F-ASWR-

DATOS DEL FUNCIONARIO SOLICITANTE

Nombres:

Unidad Administrativa:

Cargo:

DIRECCIONES ESPECÍFICAS

JUSTIFICACIÓN

El buen USO de los permisos asignados a través de este formulario, es RESPONSABILIDAD tanto del funcionario solicitante como del jefe inmediato. La Unidad de Gestión de Tecnología monitorea permanentemente el rendimiento de la red de datos e Internet y notificará cualquier novedad que atente a la seguridad de la Información.

Nombre del Funcionario: **Nombre de Jefe Inmediato:**

Firma: **Firma:**

Gobierno del Encuentro

GUILLERMO LASSO
PRESIDENTE

UNIDAD DE GESTIÓN TECNOLÓGICA

CREACIÓN / ACCESO A CARPETAS COMPARTIDAS

DATOS DE LA SOLICITUD

Fecha: _____ **No.** UGT-CACC _____

DATOS DEL FUNCIONARIO SOLICITANTE

Cédula: _____ Unidad Administrativa: _____

Nombres: _____ Cargo: _____

CARPETA COMPARTIDA

NOMBRE DE CARPETA:		**IP**	
FUNCIONARIOS:	**PERMISOS**		
	LECTURA	**LECTURA / ESCRITURA**	

JUSTIFICACIÓN

FIRMAS DE RESPONSABILIDAD

ÁREA REQUIRENTE

Nombre Solicitante: _____ **Nombre Jefe inmediato:** _____

Firma: **Firma:**

NOTA: LA FIRMA DE AUTORIZACIÓN CONLLEVA RESPONSABILIDAD EN RELACIÓN AL USO DE LOS PERMISOS CONCEDIDOS, CUALQUIER MAL USO DE ÉSTOS SERÁ NOTIFICADO PARA LOS FINES PERTINENTES.

LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS NO SE RESPONSABILIZA POR LA INTEGRIDAD DE LA INFORMACIÓN ALMACENADA EN LAS CARPETAS COMPARTIDAS

ACUERDO DE CONFIDENCIALIDAD

Yo, , identificado(a) con documento de identidad No. , como servidor/a público/a de la Secretaría Técnica Ecuador Crece sin Desnutrición Infantil (STECSDI), comprendo que durante mis labores en la institución tendré acceso a información confidencial y por esto me comprometo a no divulgar ningún tipo de información perteneciente a la STECSDI con propósitos diferentes a los descritos en mis funciones dentro de la institución.

CLÁUSULA PRIMERA. - DECLARATORIA DE CONFIDENCIALIDAD:

1. El servidor público se compromete a usar los recursos de información y tecnológicos de la STECSDI de manera legal, profesional y ética; es corresponsable solidario de mantener la misma de forma Confidencial, Íntegra y Disponible, lo que significa cumplir y hacer cumplir todos los procesos y políticas que garanticen el procesamiento seguro y confidencial de la información a la que tiene acceso dentro de sus labores profesionales.

2. El servidor público ha sido informado y acepta que la STECSDI es el titular de la información institucional, la que comprende toda la información física o digital, recibida o generada durante los procesos estratégicos, operativos y de apoyo, así como la información relacionada a la correspondencia física o virtual y que se encuentra bajo su custodia en archivos físicos temporales o permanentes, bases de datos, redes electrónicas, sistemas de información institucionales, aquella almacenada en los recursos tecnológicos a nivel de usuario; y/o, la información que se encuentren en etapa de gestión en los procesos internos.

3. El servidor público declara que ha leído el Acuerdo de Confidencialidad y acepta que la Información Institucional, es inalterable y de propiedad exclusiva de la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL, desde el momento en que le es comunicada o transferida, ya sea de manera electrónica o física, o por cualquier otro medio de comunicación que use la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL.

4. El servidor público acepta que, en atención a la naturaleza de la información y a los riesgos que el mal uso y/o divulgación de la misma implican para la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL del Ecuador, está obligado a mantener en forma estrictamente reservada toda información confidencial o reservada como tal de acuerdo a la Ley Orgánica de Transparencia y Acceso a La Información Pública (LOTAIP) en sus artículos 6, 17, 18, y demás información sensible que se le proporcione o a la que tenga acceso en función del cargo que desempeña; por lo tanto se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral o escrito, o ceder a terceros sin autorización debidamente documentada y aprobada, y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses de la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL del Ecuador.

5. El servidor reconoce que, en razón de las gestiones que realice en cumplimiento a sus labores, podría llegar a tener acceso a datos personales y que, en consecuencia, mantendrá absoluta reserva respecto de dicha información, conforme lo que establece la Ley Orgánica de Protección de Datos Personales, lo cual implica que se deberá abstener de usar, disponer, divulgar y/o publicar por cualquier medio, oral o escrito, o ceder a terceros sin autorización debidamente documentada y aprobada, y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los del propio titular y a las labores de la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL del Ecuador. La inobservancia a lo aquí detallado, será exclusiva responsabilidad del servidor público, por lo cual releva expresamente a la STECSDI de cualquier reclamación que se formulare, producto de un inadecuado o mal uso de los datos personales a los que tenga acceso.

CLÁUSULA SEGUNDA. - OBLIGACIONES:

1. Es obligación del servidor público, utilizar la información a la que tiene acceso en razón de su trabajo, únicamente para los fines legítimos y propios de sus labores y a las disposiciones del Jefe de la unidad a la que pertenece, siempre que se ciña a los fines legítimos que faculta la normativa. De igual forma, es deber del servidor público abstenerse de acceder a la información que no le haya sido autorizada, asignada o permitida, por lo cual dicha información oficial no puede, por ninguna circunstancia, ser usada para provecho o ventaja personal de los servidores públicos, sus familias o cualquier otra persona, ni en detrimento de terceros.

2. El servidor público no accederá a la información que la STECSDI recopile, genere, o de tratamiento, a menos que su cargo o función lo requiera específicamente.

3. El servidor público no debe revelar sin autorización expresa, bajo ningún medio (electrónico, verbal o físico), la información sensible que maneja la STECSDI misma que incluye pero no se limita a: información considerada como confidencial, datos personales, los planes de negocio y/o institucionales, programas, cartera de proyectos internos o externos, documentos relacionados con concursos públicos, rutinas de trabajo u otros aspectos que estén vinculados con la gestión de la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL del Ecuador.

4. La información será tratada únicamente a través de los canales de difusión autorizados, lo cuales serán definidos por la STECSDI de acuerdo a normativa vigente.

   El servidor público debe mantener especial cuidado con la información considerada confidencial o sensible a la que tenga acceso, manteniendo resguardo permanente de la misma.
5. El Servidor público se obliga a mantener una política de escritorio limpio, y guardar bajo llave la información sensible evitando que quede sin protección o sea accesible por cualquier otro servidor público, o por terceros externos a la institución no autorizados.

6. Llevar registro y control de la información sensible que esté bajo su administración y custodia.

7. El Servidor público debe informar al Jefe de la unidad a la que pertenece en caso de encontrar irregularidades en cuanto al manejo o accesos no autorizados a la información sensible o confidencial que le ha sido asignada.

8. El servidor público tiene la obligación de conocer la Política de Seguridad de la Información institucional, así como acatar las directrices que la institución expidiese en esta materia.

CLÁUSULA TERCERA. - SANCIONES:

El presente Acuerdo y su contenido representan una obligación formal de servidor público con la SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICION INFANTIL del Ecuador. Cualquier incumplimiento al mismo, se considera una falta disciplinaria, por la cual se aplicarán las sanciones establecidas en la Ley Orgánica del Servicio Público (LOSEP), Ley Orgánica de Transparencia y Acceso a La Información Pública (LOTAIP) o por el Código de Trabajo (CDT), según corresponda, sin perjuicio de las acciones civiles, administrativas y/o penales a las que hubiere lugar.

De igual manera, reconoce que cualquier daño a terceros que se ocasione con ocasión de la inobservancia a lo aquí detallado, podría generar obligaciones de indemnización, que deberán ser cubiertas por el servidor público.

CLÁUSULA CUARTA. - VIGENCIA:

Los compromisos establecidos en el presente Acuerdo de Confidencialidad tendrán vigencia a perpetuidad, con el fin de preservar la información institucional.

CLÁUSULA SÉXTA. - ACEPTACIÓN:

Para constancia de haberse participado, poner conocimiento y aprobado el contenido del presente Acuerdo de Confidencialidad por parte del servidor público(a), quien en consecuencia acepta su contenido y se compromete a su fiel cumplimiento, procede a la suscripción del mismo en conjunto con el/la Director/a conforme establece el Art. 14 inciso c) del Acuerdo No. STECSDI- STECSDI-2021-0027-A del 15 de diciembre de 2021, de Delegación De Facultades y Atribuciones para la "SECRETARÍA TÉCNICA ECUADOR CRECE SIN DESNUTRICIÓN INFANTIL", expedido por el Mgs. Erwin Rafael Ronquillo Coellar, Secretario Técnico Ecuador Crece Sin Desnutrición Infantil.

Dado en la ciudad de Quito, al día del mes de 2002

Firma: _____
Nombre:
C.C.

Nombre
DIRECTOR(A) DE ADMINISTRACION DEL TALENTO HUMANO
Delegado (a) de la Máxima Autoridad