COEPRISS
COMISIÓN ESTATAL PARA LA PROTECCIÓN CONTRA RIESGOS SANITARIOS DE SINALOA

COEPRISS SGC
SISTEMA DE GESTIÓN DE CALIDAD

LINEAMIENTOS OFICIALES EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE COEPRISS

COEPRISS-LCA-01.

CONTENIDO

1. INTRODUCCIÓN

La Comisión Estatal para la Protección Contra Riesgos Sanitarios del Sinaloa (COEPRISS), Emite los presentes lineamientos con fundamento en el artículo 54 del **Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal**, el cual faculta a las instituciones a establecer el uso compartido de comunicaciones considerando sus disposiciones los cuales a su vez deben ser contemplados en los instrumentos de colaboración y contratos de servicios de red que se celebren.

En este sentido, el lineamiento se emite para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información de COEPRISS.

Por lo anterior con los presentes lineamientos es posible contribuir a definir el uso y aprovechamiento de las tecnologías de la información, mediante criterios de legalidad, honestidad, eficacia, económica, transparencia, control y rendición de cuentas, así como coadyuvar en el aseguramiento de la TIC de la institución.

2. TÉRMINOS Y DEFINICIONES.

Acceso Físico: Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.

Acceso Lógico: Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.

Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Activo: Cualquier bien tangible o intangible, que tenga valor para la organización.

Activos de TIC: Los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Adscripción: Asignación o ubicación de una persona o unidad administrativa dentro de la estructura organizativa de la Comisión Federal.

Amenaza: Causa potencial de un incidente no deseado, que puede dar como resultado un daño a un sistema o a la organización.

Antivirus: Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.

Aplicación: Acción que se realiza a través de un programa de manera directa con el usuario, navegadores, chat, correo electrónico, etc. Son algunos ejemplos de aplicaciones en el medio de Internet.

Aplicativo de Cómputo: El software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Aptitud: Conjunto de conocimientos, experiencias, criterios, personalidad y, en general, todas las habilidades necesarias que posee un individuo para desempeñar un puesto. La aptitud es lo que determina el rendimiento global o varios aspectos de la personalidad y revela la capacidad de un individuo para adquirir mediante el entrenamiento una habilidad determinada.

Archivo: Conjunto de expedientes o documentos organizados con el fin de integrar una fuente de información en razón de las actividades de las diferentes unidades de la Comisión Federal, de acuerdo a los lineamientos establecidos por la coordinadora sectorial.

Área Crítica: Es el área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la institución ataque: Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo. Atribuciones: Facultades que se confiere a una unidad administrativa o a un puesto para ejecutar determinadas actividades. A través de las atribuciones se delimita el ámbito de competencia.

Auditoría: Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad, para asegurar el cumplimiento con la política establecida y procedimientos operativos y para recomendar cualquier cambio que se estime necesario.

Autorización: Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.

Base de Datos: Conjunto de registros cuantitativos y/o cualitativos interrelacionados.

Bienes de Consumo: Aquellos que por su naturaleza y finalidad de servicio son considerados como insumos y materias primas de proceso productivo, que pueden o no tener un uso constante y duradero.

Borrado Seguro: El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital

Capacitación: Acción destinada a desarrollar el conocimiento, las aptitudes, las actitudes y las competencias de los servidores públicos de la Comisión, con el propósito de prepararlos para desempeñar adecuadamente una ocupación o puesto de trabajo. Su cobertura abarca entre otros, los aspectos de conocimiento, atención, memoria, análisis, actitudes y valores de los individuos, respondiendo sobre todo a las áreas cognoscitivas y afectivas del aprendizaje.

Centro de Datos (SITE): El lugar físico en los que se ubiquen los activos de TIC y desde el que se provén servicios de TIC.

Comprimir: Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Zip es el nombre de la extensión que contiene un archivo comprimido.

Confidencialidad: Principio fundamental de seguridad que busca garantizar que toda la información de las personas, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

Contraseña: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe tenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se

les solicita la clave; se conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso Control de Acceso:

1. Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria.

2. Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

Correo Electrónico: La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar una computadora y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección específica a través de la red o Internet.

Cracker: Es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que, a diferencia de éste último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Cuentas de Usuario: Es un identificador único, el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Directorio Activo: son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

Disponibilidad: Principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando está es requerida por el proceso del negocio. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

Dominio Tecnológico: Las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.

Encriptación: Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encriptación como tal, no existe en el lenguaje español, el término correcto es CIFRADO DE DATOS.

Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

Equipo de Telecomunicaciones: Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Estación de Trabajo: Área destinada para que un usuario de la red pueda acceder a la misma mediante dispositivos de red (Pc's, Lap top, tablet, teléfono, etc.).

Estándar: Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

Evaluación de riesgo: Proceso global del análisis de riesgos y de la evaluación de riesgos.

Facultad: Posibilidad jurídica que tiene un sujeto de ejecutar, bajo su responsabilidad, determinados actos administrativos.

Faltas administrativas: Las Faltas administrativas graves, las Faltas administrativas no graves; así como las Faltas de particulares.

Falta administrativa no grave: Las faltas administrativas de los Servidores Públicos en los términos de la LGRA, cuya sanción corresponde a las Secretarías y a los Órganos internos de control.

Falta administrativa grave: Las faltas administrativas de los Servidores Públicos catalogadas como graves en los términos de la LGRA, cuya sanción corresponde al Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas.

Faltas de particulares: Los actos de personas físicas o morales privadas que estén vinculados con faltas administrativas graves a que se refieren los Capítulos III y IV del Título Tercero de la LGRA, cuya sanción corresponde al Tribunal en los términos de la misma.

Firewall: Normalmente conocido como barrera cortafuegos. Es un filtro en software o hardware que controla todas las comunicaciones entrantes y salientes de una red a otra red, cuya función principal es denegar o permitir el acceso de dicha comunicación. Así para denegar o autorizar una comunicación, el firewall primero analiza el perfil del usuario si tiene o no acceso a un determinado servicio tales como: acceso a Internet, correo, transferencia FTP, etc.; y luego denegará o dará paso a dicha comunicación.

Freeware (Software Libre). Programas que se pueden bajar desde Internet sin cargo.

Hacker: Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Herramientas de seguridad: Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

Impacto: Magnitud del daño ocasionado a un activo en caso de que se materialice.

Incidente de seguridad: Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.

Informática: ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y sistemas informáticos.

Integridad: Principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas de la organización, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad. La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. La información no puede ser alertada ni eliminada por cambios no autorizados o accidentales.

Internet. Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.

Intrusión: Es la acción de introducirse o acceder sin autorización a un activo.

Malware: Se define como software malicioso que cubre un amplio rango de software hostil como son los virus, gusanos, caballos de troya, etc., capaces de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.

Marco Legal: Bases jurídicas a las que debe ceñirse la Comisión Federal en el ejercicio de sus funciones, que pueden ser leyes, decretos, acuerdos, reglamentos u otros ordenamientos o normas emitidas por las autoridades competentes.

Mecanismos de seguridad o de control: Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la

probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.

b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Metodología: Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente.

Nodo: Punto principal en el cual se les da acceso a una red a las terminales o computadoras.

Open Source: Software cuyo código fuente y otros derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia de código abierto o forman parte del dominio público.

Paquetería licenciada: Aquella paquetería informática y software que para su uso y aplicación requiere del permiso formal o por escrito del proveedor.

Paquetería no licenciada: Aquella paquetería informática y software cuyo uso y aplicación no requiere ni de un permiso especifico ni de un pago.

Rack: Estante donde se instala el equipo de telecomunicaciones y/o servidores de datos.

Recursos de procesamiento de la información: Cualquier sistema de procesamiento de información, servicio o infraestructura, o las instalaciones físicas que los alojen.

Respaldo: Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Responsabilidad: Se refiere a que ésta es una habilidad de los seres humanos para reconocer y medir las consecuencias, de un incidente que realizó en plena conciencia y libertad. Por otro lado, es la persona que dirige una actividad.

Riesgo: Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.

Seguridad de la Información: Conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Conjunto de medidas técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, pudiendo además abarcar otras propiedades como la autenticidad, la fiabilidad y el no repudio.

Servicio: Es un medio de entregar valor a los clientes, al facilitar resultados que los clientes quieren lograr sin apropiarse de los costos y riesgos especificados. A veces se utiliza el término "SERVICIO" como sinónimo de servicio base, servicio de TI o paquete de servicios.

Servidor: Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas.

Software: Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

Software propietario: Cualquier software o herramienta por la cual se requiera pagar derechos para su utilización a través de una licencia.

Soporte Técnico: Servicio ejecutado para solucionar averías físicas (hardware) o lógicas (software) de equipo de cómputo, aplicaciones y accesorios. Aquí, se pueden ofrecer dos tipos de asistencia: intelectual y tecnológica. La asistencia intelectual se concreta mediante asesorías que facilitan conocimiento y aclaraciones a quienes necesitan apoyo, mientras que la asistencia tecnológica implica realizar tareas como reparaciones, revisiones y ajustes de hardware o software.

SPAM: Se define como Correo Electrónico "tipo basura" o también conocido como "correo no solicitado". Estos mensajes son normalmente enviados a través de listas de correo invisibles o grupos de noticias que bombardean con propaganda de todo tipo de productos o servicios. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.

Spyware: Software parásito que actúa como espía o secuestrador, y se auto instala en un computador sin el permiso del usuario.

Tecnologías Verdes: el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías.

Tecnologías de la Información y de la Comunicación: todo equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

TIC: Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Tratamiento de los riesgos: Proceso de selección e implementación de las medidas para modificar un riesgo.

Usuario de TIC: Término utilizado para distinguir a cualquier persona que utiliza bienes o servicios de Tecnologías de la información y de la Comunicación dentro de la red institucional de la Coepriss.

3. Objetivo.

Establecer las políticas de uso y disposiciones para impulsar el uso y aprovechamiento de las tecnologías dela información y comunicación **(TIC)** en la **COEPRISS** con el objetivo de prevenir, detectar y/o corregir de la mejor manera cualquier problema que amanece a los activos de la Institución o a la disponibilidad, integridad de la información de la comisión.

4. Alcance.

Las presentes políticas son aplicables a todos los procesos, a la infraestructura de las tecnologías de la información y de la comunicación, así como a los activos de información y deberán ser observadas por todos los usuarios que utilicen los servicios de los activos y la red institucional (voz, datos y videoconferencia) de la **COEPRISS**,

Para los casos no previstos en el presente documento serán resueltos por el área de **GESTIÓN DE CALIDAD**.

5. Normatividad Aplicable.

1.1. Ley Orgánica de la Administración Pública Federal
DOF 03-05-2023 Articulo 8 y sus reformas publicadas.

1.2. Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la administración pública federal.
DOF: 06/09/2021
Artículo 54.
Artículo 57.
Artículo 75.

1.3. Ley Orgánica de la Administración Pública Federal
DOF 03-05-2023 Articulo 8 y sus reformas publicadas.

1.4. Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa
P.O. 54 del 4 de mayo de 2016. y sus reformas aplicables.
Artículo 33.
Artículo 34.

1.5. Ley de Protección de Datos Personales en posesión de sujetos obligados del Estado de Sinaloa.
AP-CEAIP004/2019.

1.6. Ley de Austeridad del Estado de Sinaloa.
Capítulo 6 fracción IV.

1.7. Ley Federal de Derechos de Autor
DOF 20-Ago-15
Artículo 103.
Artículo 105.

1.8. ACUERDO por el que se expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones.
Artículo 4.

6. Disposiciones Generales.

1.9. El ejercicio control de la información y comunicación, así como los activos de la información que utilicé el personal de **COEPRISS** deberá sujetarse a las disposiciones que establezca el Comisionado Estatal de la Comisión Estatal para la Protección Contra Riesgos Sanitarios de Sinaloa **(COEPRISS)** así como el responsable de informática de **COEPRISS.**

1.10. La política general de seguridad de la información está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional.

Del uso del correo electrónico a través de dispositivos móviles

1.11. Los diversos sitios geográficos que cuentan con infraestructura de red para efectos de administración se identificaran como nodos, la ubicación de los mismos puede ser local o remota en las entidades federativas.

1.12. La red institucional (voz, datos y videoconferencia) está conformada por la infraestructura de telecomunicaciones necesaria para proporcionar de manera local y/o remota servicios en materia de **(TIC)** al personal de la **COFEPRIS** para desempeñar sus funciones.

Del Personal de la Unidad Administrativa (UA).

1.13. En concordancia con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados Articulo 2 3 4 5 6 7 las personas físicas o morales que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, serán responsables de los datos personales, y se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

1.14. Mantener, Proteger los activos de la información de la UA perteneciente en buen estado.

1.15. Los datos de carácter personal que sean recabados para incorporarse a una base de datos, deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma, e informarse al titular en el momento en que la información personal es recolectada.

1.16. No deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando con ello la protección de los intereses del titular y la expectativa razonable de privacidad.

1.17. Se entenderá que el responsable actúa de forma engañosa o fraudulenta cuando:

I. Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo.
II. Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular.
III. III. Vulnere la expectativa razonable de protección de datos personales.

1.18. Las instituciones deberán, ante el uso compartido de redes de comunicaciones, considerar al menos los siguientes elementos:
a) Mecanismos y políticas de seguridad.
b) Protocolos de actuación en contingencias.
c) Niveles de servicios.
d) Identificación de vulnerabilidades.
e) Requisitos de gestión de todos los servicios de red.

Los cuales deberán estar contemplados en los Instrumentos de colaboración y contratos de servicios de red que se celebren.

1.19. El personal que labora en **COEPRISS**, podrá solicitar apoyo al personal de Informática, para que realice la configuración del correo electrónico institucional en el dispositivo móvil.

Del departamento de Informática.

1.20. El personal de la Informática no realizará ningún tipo de respaldo de información, ni de contactos en los dispositivos de los usuarios.

1.21. Administrar y supervisar que en los servicios se realicen al menos las siguientes tareas.

a) Identificar la infraestructura crítica de este servicio, así como el rol específico de la función que realiza en la red.
b) Identificar el direccionamiento especifico de los componentes de la infraestructura física con el fin de facilitar el diagnostico en caso de fallas.
c) Validar el correcto funcionamiento de los servicios de la LAN en los casos de implementación, fallas, cambios.
d) Monitorear el desempeño de los servicios.
e) Validar los niveles de servicio acordados.
f) Gestionar el acceso a los servicios de red para los usuarios y/o dispositivos que requieran acceso, tales como; servidores, checadores, Access Point, etc.

1.22. Supervisar que se realicen al menos las siguientes tareas en las diversas etapas de implementación, migración, operación, control de cambios, etc.:

a) Infraestructura de red
b) Licenciamiento
c) Monitoreo

De los servicios necesarios para la operación de acuerdo a la normatividad y/o contrato vigente.

1.23. La implementación de todos los servicios de plataformas digitales de páginas web que realice la COEPRIISS, el departamento de informática deberá observar, al menos lo siguiente:

a) Considerar la aplicación de los Estándares Técnicos en materia de arquitecturas de desarrollo e interoperabilidad, y servicios de hospedaje.
b) Aplicar las mejores prácticas para el desarrollo de plataformas web, como los estándares y recomendaciones del Consorcio de la Red Informática Mundial (W3C, World Wide Web Consortium) relativos a uso de lenguajes de marcado, hojas de estilo, accesibilidad web y validadores.
c) Compatibilidad con todos los navegadores actuales y de nuevas generaciones, así como con sistemas operativos móviles y sus navegadores;

d) Contar con versiones de páginas web adaptables a las resoluciones de dispositivos móviles.
e) Incluir funciones de accesibilidad para personas con discapacidad, de conformidad con los Estándares Técnicos de la CEDN.
f) Incluir Aviso de privacidad, así como términos y condiciones de uso claros y actualizados, en los términos de la legislación aplicable.
g) Garantizar que el acceso a las plataformas digitales de páginas web se realice a través de mecanismos de autenticación y cifrado mediante certificados digitales.

1.24. Clasificará el incumplimiento de las presentes políticas como:

- No grave: Aquella falta que por su naturaleza no afecte al desempeño de las actividades de la COEPRISS.
- Grave: Aquella falta, que afecte los procesos críticos de la COEPRISS, pero se hayan identificado en tiempo y sea posible revertir su afectación.
- Muy grave: Aquella falta, que afecte los procesos críticos de la COEPRISS y hayan causado alguna afectación irreparable a la operación.

Las acciones que se enuncian a continuación ejemplifican posibles infracciones a las TIC´S.

Acciones de mal uso de la infraestructura de red y/o activos informáticos y tecnológicos:

a) Hacer uso de la red de datos, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.
b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica de la Comisión.
c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Comisión.
d) Conectar equipos de cómputo personal, switches u otros sistemas electrónicos personales a la red de datos de la Comisión, sin la debida autorización.
e) El utilizar los recursos tecnológicos de la Comisión para beneficio personal.
f) Instalar programas o software no autorizados en los Equipos de cómputo, cuyo uso no esté autorizado por la Dirección de Ejecutiva de Sistemas y Procesos.

Acciones de sabotaje de la infraestructura de red y/o activos informáticos.

a) Impedir u obstaculizar el funcionamiento a los aplicativos, bases de datos o a las redes de telecomunicaciones y datos de la Comisión, sin estar autorizado.
b) Destruir, dañar, borrar, deteriorar activos informáticos de la Comisión, sin autorización.

c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la Comisión.
d) Alterar datos personales de las bases de datos propiedad de la Comisión.
e) Realizar cambios no autorizados en la plataforma tecnológica de la Comisión.

Acciones de acceso no autorizado a la infraestructura tecnológica.

a) Acceder sin autorización expresa a todo o en parte a los sistemas de la COEPRISS.
b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.
c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la COEPRISS o permitir que otras personas accedan con el usuario y clave del titular a éstos.
d) Otorgar el acceso o privilegios a la infraestructura de la COEPRISS a personas no autorizadas.
e) Ingresar a carpetas sin autorización.

Acciones de robo de información.

a) Ejecutar acciones tendientes a eludir o variar los controles establecidos por de la COEPRISS.
b) Retirar de las instalaciones de la COEPRISS, equipos de cómputo que contengan información de la COEPRISS, sin la autorización pertinente.
c) Sustraer de las instalaciones de la COEPRISS documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.
d) Entregar, enseñar y divulgar información institucional, a personas o entidades no autorizadas.
e) Copiar sin autorización los programas de la COEPRISS o violar los derechos de autor o acuerdos de licenciamiento.

Sanciones.

a) El incumplimiento a las presentes políticas y que se encuentre en alguno de los supuestos antes mencionados, será sancionado con una llamada de atención por escrito o correo electrónico al usuario y se hará del conocimiento de su jefe inmediato.

b) Si el usuario incurre en el uso no autorizado de los servicios de red, se cancelará el mismo; así mismo, si hace un mal uso de los recursos de red (Internet, correo electrónico), comunicación telefónica (local, celular y larga distancia) se suspenderá temporalmente el servicio, reanudándose hasta el momento en que, de manera escrita, sea solicitado por su jefe inmediato. Con la consigna de que la reincidencia en el abuso se considerará como una falta grave y se procederá conforme a la misma.

7. Control de cambios.

Versión	Fecha	Elaboró	Firma	Descripción del cambio
2	12/02/2025	**Lic. Cosme Verduzco Bojórquez** Responsable del Área de Informática		Se modifico el formato del proceso, así como los logos y se añadió a revisión a la coordinadora administrativa.
		Revisó	**Firma**	
		Lic. Ricardo Anibal Garcia Reyes Responsable del SGC		
		Revisó	**Firma**	
		Lic. Beatriz Aguiar Monroy Encargada de la Coordinación Administrativa	Beatriz Aguiar M.	
		Aprobó	**Firma**	
		Lic. Cuauhtémoc Chacón Mendoza Comisionado Estatal de COEPRISS		

8. Anexos.

Anexo 1.- Formato para entrega y resguardo de equipos de cómputo y accesorios.

SALUD **FORMATO DE ENTREGA Y RESGUARDO** c epriss

Fecha de Elaboración:	Tipo de Movimiento:
02/01/2024 13:30	Resguardo
Área Emisora:	**Folio de Resguardo:**
Administración-Informatica	INF-312

Ubicación Actual

Coordinación:	OFICINA CENTRAL	Departament	OFICINA CENTRAL
Domicilio Completo:	SERVICIOS DE SALUD DE SINALOA		

Resguardo

Nombre:	Puesto:
COSME VERDUZCO BOJORQUEZ	INFORMATICA

Características del Equipo

Descripción

LAPTOP HACER W700 G1T. I7. 16 GB RAM. 500 GB DD SOLIDO

Adaptador de LAN Inalámbrica:	Adaptador de Ethernet
Integrado	Integrado

Descripción del PS Entregado

Descripción	Marca	Modelo	No. Serie	Inventario
LAPTOP HACER W700 G1T. I7. 16 GB RAM. 500 GB DD SOLIDO	ACER	W700	NXVPNAL003 1342DF9F760 0	S/N
Observación:	EQUIPO NUEVO			

Firmas de Entrega y Regulado del PS

Entrega del Equipo	Recibe de aceptación y Conformidad	Enlace de gestión administrativa de COEPRISS
COSME VERDUZCO BOJORQUEZ	COSME VERDUZCO BOJORQUEZ	BLANCA ARIANA PLATA ERICON
Nombre y Firma del Quien Entrega	Nombre y Firma del Usuario Responsable	Nombre y Firma Area Administrativa (Vo. Bo.)

Como usuario acepto la responsabilidad de conservar los bienes señalados en el presente resguardo, en óptimas condiciones físicas durante mi estancia en esta unidad administrativa, así como hacer entrega de éstos ante la autoridad correspondiente, en cuanto me sea solicitado, o bien, en cuanto concluya en cargo que desempeño, así mismo, acepto toda responsabilidad del contenido de todos los archivos que se encuentren en este equipo a partir de esta fecha, y reconozco que es mi deber informar por escrito a mis superiores si tengo conocimiento de alguna irregularidad en este equipo, a fin de que se tomen las medidas procedentes. Me comprometo a realizar todas las siguientes administrativas y legales en caso de robo o extravío de este equipo, y con mi firma en Usuario Responsable, acepto recibir copia de este formato de resguardo de equipo.

Anexo 2.-Formato de Dictamen técnico para baja de equipos de cómputo y accesorios.

SERVICIOS DE SALUD DE SINALOA
OFICINA ADMINISTRATIVA
SISTEMAS

SERVICIOS DE SALUD SINALOA

c epriss

DICTAMEN TECNICO

COEPRISS

CULIACÁN, SIN. 02/01/2024 FOLIO COE-CENTRO-10-2022-080

DATOS GENERALES DEL EQUIPO

EQUIPO	NO-BREAK PILA	No. DE INVENT.	
MARCA	ISB	AREA:	COEPRISS
MODELO	XRN-21-4B1	CLAVE DEL BIEN :	
N/S	E14K04143		

DESCRIPCION OPERACIONAL Y/O FUNCIONAL

NO MANTIENE CORRIENTE, PILAS DAÑADAS, SE APAGA

OBSERVACIONES .

CONDICIONES TECNICAS

NO SE CONSIGUEN REFACCIONES	X	NO PASA PRUEBA DE SEGURIDAD	X
OBSOLETO	X	NO NECESITA SERVICIO	
FALTAN ACCESORIOS		INFORMACION INCOSTEABLE	X
REPARABLE		FALTA DE REFACCIONES	

ESTADO FISICO DEL EQUIPO

MALO

DISPOSICION RECOMENDADA DEL EQUIPO

REPARACION		DONACION	
PERMANENCIA		BAJA	X
REUBICACION		STOCK DE REFACCIONES	

DICTAMINO

LEOBARDO DE LA HERRAN VILLAPUDUA
SOPORTE

DICTAMINO

COSME VERDUZCO BOJORQUEZ
INFORMATICA COEPRISS

ATENTAMENTE

LIF. JORGE ARMANDO SOTO MEDRANO
JEFE DE SISTEMAS