Políticas para uso de Bienes y Servicios Informáticos

POLÍTICAS PARA USO DE BIENES Y SERVICIOS INFORMÁTICOS

Índice

Objetivo General y Específicos 1

Marco Legal 2

Responsabilidades 7

Políticas para uso de Bienes y Servicios Informáticos 8

- **Uso de los bienes informáticos** 8
- **Uso de Internet** 12
- **Sistemas de Información** 14
- **Uso de la Red de Voz y Datos** 15
- **Uso del correo electrónico** 17

Cumplimiento 19

Sanciones 20

Glosario 21

Objetivo General y Específicos

Objetivo General

Coadyuvar a mantener la confiabilidad, seguridad, disponibilidad e integridad de la información, así como un mayor aprovechamiento de los recursos informáticos y de comunicaciones propiedad de la Institución, lo cual contribuirá de manera determinante a aumentar la eficiencia en el trabajo, en apoyo al cumplimiento de la misión institucional.

Objetivos Específicos

- Utilizar los recursos tecnológicos de información y comunicaciones al servicio o propiedad de la Institución, en forma responsable y apropiada, de conformidad con las políticas descritas en el presente manual y otras de carácter institucional, así como lo especificado en la normatividad aplicable en la materia.

- Minimizar las interrupciones en la disponibilidad de los servicios asociados a los sistemas informáticos y de comunicaciones, ocasionados por el uso inapropiado o por daños causados de forma accidental o intencional.

- Contribuir a mantener los equipos y accesorios en óptimo estado, maximizando su vida útil. Contribuyendo a que la inversión en tecnología se dé en función de calidad, desempeño del equipo y garantía.

Marco Legal

Las presentes **Políticas para el Uso de Bienes y Servicios Informáticos** tienen por objeto establecer las disposiciones institucionales aplicables al uso, asignación, administración, protección, conservación, control y, en su caso, baja de los bienes y servicios informáticos de la Secretaría de Salud del Estado de Baja California Sur y del Instituto de Servicios de Salud de Baja California Sur.

Su fundamento jurídico se integra exclusivamente por las disposiciones estatales que guardan relación directa con el uso y administración de equipos de cómputo y dispositivos móviles institucionales, correo electrónico, acceso a Internet, redes y servicios de telecomunicaciones, cuentas y mecanismos de autenticación, software y licenciamiento, sistemas de información, respaldos, seguridad informática, protección de datos personales, gestión de documentos electrónicos, inventario y baja de bienes informáticos.

Para tal efecto, resultan aplicables, en lo conducente, las siguientes disposiciones:

I. Constitución Política del Estado Libre y Soberano de Baja California Sur

Artículo 13, apartado B, en las disposiciones relativas al derecho de toda persona a la protección de sus datos personales y a los derechos de acceso, rectificación, cancelación y oposición, así como a los principios y bases que deben observar las autoridades estatales en materia de protección de datos personales.

II. Ley de Responsabilidades Administrativas del Estado y Municipios de Baja California Sur

Artículo 7, fracción VI, respecto de la obligación de las personas servidoras públicas de administrar los recursos públicos que se encuentren bajo su responsabilidad, sujetándose a los principios de eficiencia, eficacia, economía,

transparencia y honradez y destinándolos al cumplimiento de los objetivos para los cuales fueron asignados.

Artículo 49, fracción V, respecto de la obligación de registrar, integrar, custodiar y cuidar la documentación e información que, por razón del empleo, cargo o comisión, se encuentre bajo responsabilidad de la persona servidora pública, así como de impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos.

Artículo 50, respecto de los daños y perjuicios que, de manera culposa o negligente, se ocasionen a la Hacienda Pública o al patrimonio de un ente público.

Artículos 53 y 54, en lo relativo al uso, apropiación, asignación o desvío indebido de recursos públicos, incluidos los recursos materiales.

Las disposiciones anteriores constituyen fundamento para establecer responsabilidades institucionales respecto del uso, custodia, conservación y aprovechamiento de equipos de cómputo, dispositivos móviles, periféricos, sistemas, cuentas, redes, software, licencias, servicios tecnológicos y demás recursos informáticos institucionales.

III. Ley de Bienes del Estado de Baja California Sur

Artículo 27, respecto de la integración de los inventarios de los bienes del dominio público y privado estatal.

Artículo 28, respecto de la obligación de los entes públicos y entidades de la Administración Pública Estatal que utilicen, administren o tengan bajo su cuidado bienes del Estado de formular los inventarios respectivos y mantenerlos actualizados.

Artículo 53, respecto del procedimiento aplicable cuando un bien mueble deje de ser necesario para el servicio del Estado o, por sus condiciones de uso, deba ser sustituido, sujetándose a las normas aplicables en materia de registro, afectación, baja y disposición final de bienes muebles.

Estas disposiciones constituyen fundamento para el registro, identificación, asignación, resguardo, control, actualización de inventarios, sustitución y baja de equipos de cómputo, teléfonos celulares, dispositivos de comunicaciones, periféricos y demás bienes informáticos que formen parte del patrimonio institucional.

IV. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California Sur (Boletín del 24 de diciembre de 2025)

Artículo 3, particularmente las definiciones relativas a bases de datos, cómputo en la nube, datos personales, datos personales sensibles, documento de seguridad, medidas de seguridad administrativas, físicas y técnicas, sistemas de tratamiento y demás conceptos relacionados.

Artículo 4, respecto de la aplicación de la Ley al tratamiento de datos personales contenidos en soportes físicos, electrónicos o cualquier otro formato, independientemente de su forma de creación, procesamiento, almacenamiento u organización.

Artículo 25, respecto de la obligación de establecer y mantener medidas de seguridad administrativas, físicas y técnicas que garanticen la confidencialidad, integridad, disponibilidad y protección de los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.

Artículo 26, respecto de los factores que deben considerarse para determinar las medidas de seguridad, incluyendo el riesgo, sensibilidad de los datos, desarrollo tecnológico, consecuencias de una vulneración y transferencias de datos personales.

Artículo 27, respecto de la obligación de crear políticas internas de gestión y tratamiento, definir funciones y obligaciones del personal, elaborar inventarios de datos personales y sistemas de tratamiento, realizar análisis de riesgos y brechas, establecer planes de trabajo, monitorear las medidas de seguridad y capacitar al personal.

Artículo 28, respecto de la documentación e integración de las acciones de seguridad en un sistema de gestión.

Artículo 29, respecto del contenido mínimo del documento de seguridad, incluyendo el inventario de datos personales y sistemas de tratamiento, funciones y obligaciones del personal autorizado, análisis de riesgos y brechas, plan de trabajo y mecanismos de monitoreo y revisión.

Artículos 30 y 31, respecto de la actualización del documento de seguridad y de la implementación de acciones preventivas y correctivas ante vulneraciones.

Artículos 32 a 35, respecto de las vulneraciones de seguridad, su registro, atención, acciones correctivas y comunicación cuando corresponda.

Artículo 36, respecto de la obligación de establecer controles para garantizar la confidencialidad de los datos personales por parte de las personas que intervengan en cualquier fase de su tratamiento, incluso después de concluida su relación con el responsable.

Artículos 52 y 53, respecto de las obligaciones de las personas encargadas del tratamiento de datos personales y de las medidas de seguridad, confidencialidad, notificación de vulneraciones y supresión o devolución de datos que deben contemplarse en los instrumentos jurídicos correspondientes.

Artículos 57 y 58, respecto de la contratación y utilización de servicios, aplicaciones e infraestructura de cómputo en la nube, incluyendo las condiciones de seguridad, confidencialidad, restricción de accesos y supresión de datos al término del servicio.

Las disposiciones anteriores constituyen el fundamento principal para establecer reglas institucionales sobre contraseñas y mecanismos de autenticación, perfiles y privilegios de acceso, seguridad de equipos y dispositivos, configuración de software y hardware, redes, almacenamiento, respaldos, sistemas de información, servicios en la nube, atención de incidentes y protección de datos personales.

Las medidas específicas establecidas en estas Políticas, tales como requisitos de contraseñas, bloqueo de sesión, autenticación, actualización de software, antivirus, respaldos, cifrado, controles de acceso y gestión de incidentes, deberán entenderse

como **medidas institucionales de seguridad adoptadas para dar cumplimiento a las obligaciones legales**, y no como requisitos expresamente enumerados con esa denominación en la Ley.

V. Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur

Artículo 196, fracción IV, respecto de la sanción por incumplimiento de las obligaciones establecidas en la materia de la presente ley;

“Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, conforme a las facultades correspondientes, la información que se encuentre bajo la custodia de los sujetos obligados y de sus personas servidoras públicas o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión”

VI. Ley de Archivos para el Estado de Baja California Sur

Artículos 42 y 43, respecto de los mecanismos y procedimientos para la gestión documental electrónica, incluyendo incorporación, acceso, seguridad, almacenamiento, uso, trazabilidad, generación, administración, control y migración de formatos electrónicos.

Artículos 44 y 45, respecto de la preservación a largo plazo y de las medidas organizativas, técnicas y tecnológicas para garantizar la recuperación y preservación de los documentos de archivo electrónico producidos y recibidos, incluyendo los contenidos en sistemas automatizados, bases de datos y correos electrónicos.

Artículos 46 y 47, respecto de los sistemas automatizados para la gestión documental y administración de archivos y los repositorios electrónicos.

Artículos 48 a 50, respecto de la conservación de documentos de archivo aun cuando hayan sido digitalizados y de la protección de los sistemas automatizados, documentos electrónicos y firma electrónica frente a la obsolescencia tecnológica.

Artículos 61 a 63, respecto de los servicios de resguardo proporcionados por terceros, la utilización de servicios de nube, los controles de seguridad y privacidad, la ubicación de servidores e información, los respaldos, la interoperabilidad y la conexión con redes y sistemas institucionales.

Estas disposiciones resultan aplicables al correo electrónico institucional cuando éste contenga documentos de archivo, a los sistemas de gestión documental, repositorios electrónicos, respaldos y demás medios tecnológicos utilizados para generar, recibir, administrar, conservar o preservar documentos institucionales.

Responsabilidades

Responsable	Responsabilidad
Grupo de Trabajo de Tecnologías de la Información	El Grupo de Trabajo debe revisar y proponer para su consideración a los responsables de la seguridad de la información, las políticas de seguridad y de buen uso de los bienes informáticos que considere convenientes. Así como monitorear cambios significativos en los riesgos que afectan a los recursos de la Información en la Institución.
Subdirección de Tecnologías de la Información	La Subdirección de Tecnologías de la Información es la encargada de la supervisión de las políticas plasmadas en el presente documento (salvo áreas pertenecientes al área de COEPRIS).

Responsable	Responsabilidad
Unidad de Sistemas de Información	Para las áreas que comprende la Comisión Estatal para la Protección contra Riesgos Sanitarios (COEPRIS) le corresponde a la Unidad de Sistemas de Información (USI), el seguimiento y vigilancia de las políticas.
Usuarios	Las políticas contempladas en el presente manual aplican a todos los usuarios de equipos, recursos y servicios informáticos, sean propiedad o estén al servicio de la Institución, ya sea en forma individual, compartida, que estén aislados o interconectados a las redes de voz y datos. Todos los usuarios de la Institución están obligados a cumplir las presentes políticas.

Políticas para uso de Bienes y Servicios Informáticos

Uso de los bienes informáticos

- El personal usuario de bienes informáticos es responsable del resguardo, uso, custodia y protección de los bienes asignados para el desempeño de sus funciones y tiene la obligación de cuidarlos y mantenerlos en buen estado de uso y conservación, salvo el deterioro causado por su uso en condiciones normales de operación y por el transcurso del tiempo.

- La persona resguardante del bien informático debe informar al área correspondiente sobre el robo, extravío o daño del equipo asignado, ya sea por accidente, descuido o negligencia; a la Subdirección de Tecnologías de la

Información para el Instituto o a la Unidad de Sistemas de Información para COEPRIS.

- El usuario es responsable de seguir las políticas de seguridad y procedimientos para el uso de los servicios y recursos informáticos, evitando cualquier práctica o uso inapropiado que los pudiera poner en peligro y ser un riesgo para la información de la Institución.

- Toda la información que se almacene en cualquier equipo de cómputo institucional, o bien se procese en éste, así como el resultado que se obtenga, se considera información institucional.

- Queda prohibido utilizar los discos duros de las computadoras para almacenar archivos de pornografía, música en cualquier formato, juegos o similares.

- Ante cualquier falla que presente el equipo de cómputo o periférico, el usuario notificará al área técnica a través de la mesa de ayuda. Asimismo, podrá solicitar un mantenimiento preventivo periódicamente.

- Toda adquisición de bienes y servicios informáticos, así como accesorios, refacciones de cómputo y telefonía solicitada a la Subdirección de Recursos Materiales, debe ser validada y autorizada por el área Técnica correspondiente.

- Queda prohibido que personas ajenas hagan uso de equipos o dispositivos pertenecientes o al servicio de la Institución.

- Se considera uso indebido utilizar los recursos para fines particulares durante el horario laboral.

- Toda donación o comodato de bienes y servicios informáticos debe notificarse previamente al área técnica correspondiente.

- En caso de que el equipo de cómputo donado o en comodato cuente con licencias de paquetería o de sistema operativo, se deberá enviar al área Técnica correspondiente una copia de estas, así como de las facturas respectivas.

- El usuario responsable del equipo debe informar en caso de que se realice la transferencia del mismo a fin de mantener actualizado el inventario de equipo para efectos de mantenimiento correctivo y preventivo.

- Para dar de baja equipo de cómputo, el responsable del equipo debe solicitar la baja, para que sea evaluada y reciba el dictamen correspondiente.

- Queda prohibido que los usuarios remuevan o agreguen componentes tanto de software como de hardware a los equipos de cómputo. En caso de requerir algún cambio deberá solicitarse.

- La configuración de los equipos no deberá ser modificada por los usuarios ni por personal ajeno a la Institución.

- Los usuarios de equipo informático de uso compartido son responsables de éste, del uso que se le dé a la cuenta de correo electrónico y, en su caso, del acceso a internet.

- Las licencias de paquetería de software deben ser resguardadas por la Subdirección de Tecnologías de la Información quien proporcionará una etiqueta indicando el número de licencia que le corresponde a cada equipo, misma que el

usuario debe mantener permanentemente, asimismo por la Unidad de Sistemas en caso de áreas de la COEPRIS.

- Queda prohibido utilizar los recursos para llevar a cabo actividades que se consideran fuera de la ley.

- No se debe utilizar los recursos sin respetar las disposiciones en materia de derechos de autor aplicables a textos, elementos multimedia (gráficos, fotografías, videos, música, etc.), datos y software.

- Es responsabilidad de los usuarios actualizar parches del sistema operativo, permitir su descarga automática y el reinicio del equipo de así requerirse.

- Es responsabilidad del usuario de cada equipo verificar que el software antivirus institucional se encuentre en ejecución y vigente de forma permanente. También debe de permitir el análisis completo programado mensualmente. Este análisis se agenda durante los últimos días del mes y se ejecuta al inicio de la sesión del siguiente día hábil.

- Todo usuario es responsable de mantener respaldos de su información de acuerdo a sus necesidades, en caso de las aplicaciones cliente-servidor, el responsable de los respaldos de las bases de datos es el administrador del sistema.

- Para reducir o eliminar riesgos y daños en los bienes informáticos bajo su resguardo, el personal usuario debe observar las acciones siguientes:
    - Vigilar que los equipos de cómputo se encuentren instalados en lugares adecuados y seguros.
    - Mantener conectados los equipos a las instalaciones eléctricas destinadas a estos, sin compartirlos con otros dispositivos electrónicos.
    - Apagar el equipo de cómputo al término de la jornada laboral.

- Evitar obstruir las salidas de ventilación de los equipos.
- Permitir que se realicen los servicios de mantenimiento preventivo y correctivo, así como la actualización de los sistemas operativos.
- Reportar a la Mesa de Ayuda las fallas o desperfectos que presente el equipo, dando seguimiento al reporte hasta su total desahogo.
- Participar en la capacitación del uso y manejo del Software institucional y en su caso, del Software de aplicación específica, asignados para el desarrollo de sus funciones.
- Entregar al término de su relación laboral o contractual, o ante un cambio de adscripción, los bienes informáticos asignados para su resguardo.

Uso de Internet

- Todo servicio de internet debe ser habilitado para brindar cobertura al mayor número de usuarios posibles, garantizando una adecuada disponibilidad de servicio.

- El usuario tendrá acceso a los servicios de internet conforme al perfil que se le asigne, con características de acceso, privilegios y restricciones específicas.

- El uso de internet es únicamente para actividades relacionadas con las funciones institucionales.

- No está permitido el uso de Internet para acceder a redes sociales, sitios de descarga de archivos, películas, música, fotografías o cualquier otro contenido que vulnere los derechos de autor.

- No está permitido utilizar internet para consulta de páginas con contenidos pornográficos.

- No está permitido utilizar internet para acceder a sitios que transmitan estaciones de radio o televisión, sitios recreativos, deportivos, de juegos, chistes, redes sociales o de entretenimiento o variedades, salvo en la Unidad de Comunicación Social y para el personal investigador del área COEPRIS, cuando así lo requieran sus funciones.

- El personal usuario es responsable del buen uso del servicio de acceso a Internet, por lo que debe abstenerse de:

  - Participar en pláticas interactivas (chats), foros o juegos en línea no institucionales.
  - Ingresar a sitios relacionados con entretenimiento, apuestas, juegos, compras, material con contenido sexual, comunidades virtuales de hackers, terrorismo, o bien, que promuevan el racismo o la violencia, entre otros.
  - Enviar información propiedad de la Secretaría a través de servicios de correo electrónico diferentes del institucional, como Gmail, Yahoo!, Hotmail, etc.
  - Descargar cadenas, virus, códigos maliciosos o cualquier tipo de Software.
  - Hacer uso de servicios de unidades de disco (almacenamiento) en Internet o en la nube no contratados o autorizados por la Institución.
  - Realizar o intentar cualquier actividad con fines ilícitos como accesos no autorizados, escaneos, robo, bloqueo o daño de información, sobrecarga o deterioro de los servicios informáticos, redes y sistemas de terceros.
  - Vulnerar o intentar vulnerar la seguridad de la plataforma tecnológica de la Institución utilizada para proporcionar el servicio de internet. Dentro de estas actividades se incluyen las siguientes, de manera enunciativa, mas no limitativa:
    - Monitorear el tráfico de la red y acceso a Internet.
    - Evadir o evitar los sistemas de seguridad y control con el propósito de obtener accesos no autorizados en el uso de Internet.

- Vulnerar las aplicaciones informáticas, sistemas de telecomunicaciones o redes de la Institución asociadas con el control de uso de Internet.
- Evadir cualquier medida de seguridad o las rutinas de validación y autenticación de usuarios en la red y en los sistemas de información de la Institución asociados con la plataforma tecnológica utilizada para proporcionar el servicio de Internet.

Sistemas de Información

- Todos los sistemas desarrollados o adquiridos con recursos de la Institución son propiedad de la Institución, respetando la propiedad intelectual de los mismos.

- Toda solicitud de creación de un sistema de información deberá ser presentada por vía oficial por el área requirente al área técnica correspondiente. Será responsabilidad del área solicitante gestionar los recursos presupuestales necesarios para llevar a cabo el proyecto de automatización.

- El área técnica correspondiente, conjuntamente con el responsable de la operación del sistema de información, debe establecer los niveles de seguridad necesarios en la aplicación.

- El responsable de la operación del sistema de información debe establecer por escrito los usuarios y sus niveles de permisos de acceso a la aplicación.

- Queda prohibido distribuir datos o información confidencial de la Institución sin autorización.

- Para todo requerimiento de automatización, la subdirección solicitante deberá designar a un responsable con amplio conocimiento del proceso o procesos sobre los cuales se va a trabajar para la definición de requerimientos.

- Para el personal usuario queda prohibido:
    - Distribuir o reutilizar el Software institucional en equipos distintos de los asignados para el desempeño de su encargo, conforme a las licencias de uso.
    - Modificar o recodificar el Software instalado.
    - Instalar cualquier Software adicional (comercial, shareware, freeware, etc.), sin autorización.
    - Instalar en el equipo institucional licencias adquiridas o desarrolladas por las personas usuarias.

Uso de la Red de Voz y Datos

- Cuando se realice la contratación para la instalación de cableado estructurado, este deberá supervisarse de acuerdo con los estándares nacionales e internacionales vigentes y contar con memoria técnica y una garantía mínima de 10 años.

- El usuario tendrá acceso a los servicios de la red local conforme al perfil que se le asigne, con características de acceso, privilegios y restricciones específicas.

- Las contraseñas de usuario serán entregadas personalmente a cada usuario. El manejo seguro de toda contraseña es responsabilidad del usuario.

- No se deben compartir las contraseñas personales.

- Queda prohibido suplantar a otras personas, haciendo uso de una falsa identidad, utilizando cuentas de acceso ajenas a los servicios.

- La contraseña deberá ser cambiada por el usuario por lo menos cada 6 meses y deberá tener una longitud mínima de 8 caracteres.

- Las contraseñas o passwords deben contener al menos tres tipos de caracteres, entre los siguientes:
    - Letras mayúsculas.
    - Letras minúsculas.
    - Números en sustitución de letras (1 por I, 0 por O, 3 por E, etcétera).
    - Caracteres especiales no alfanuméricos, como signos de puntuación.

- No emplear la opción “Recordar contraseña” que ofrecen algunas aplicaciones.

- Para el caso de la información alojada en los servidores con carácter de pública, no se realizan respaldos de esta, el usuario es responsable de lo que se aloja en el entendido de que cualquier usuario de red tiene los permisos para eliminar dicha información.

- Es responsabilidad de los usuarios de la red de la Institución, el contenido de la información que se almacena en los directorios creados por subdirección y/o departamento. Estos solo deben contener información de carácter institucional, no está permitido el almacenamiento de fotos personales, cadenas motivacionales, películas, música o cualquier otro tipo de archivo diferente a los generados por el desarrollo de sus funciones.

- Queda prohibido deshabilitar o desinstalar herramientas de monitoreo, software antivirus, firewall, así como cualquier otro elemento de seguridad que los equipos requieran para su correcta administración y seguridad.

- Queda prohibido intentar evitar los mecanismos de seguridad de la red o de controles impuestos, con la finalidad de perjudicar la funcionalidad de la red, o saltarse las restricciones establecidas por los administradores de la red.

- Queda prohibido dejar sesiones de trabajo abiertas.

- Todo usuario respetará la naturaleza confidencial del acceso de un usuario o cualquier otra información que pueda caer en su poder, bien como parte de su trabajo o por accidente.

- Toda responsabilidad derivada del uso de un nombre de usuario distinto al propio recaerá sobre aquel usuario al que corresponda el nombre indebidamente utilizado.

- En caso de que el usuario cambie de funciones o de área, podrá utilizar la cuenta inicialmente asignada, pero deberá comunicarlo al administrador de la red para que se realicen los ajustes necesarios.

Uso del correo electrónico

- El correo electrónico es una herramienta para el desarrollo y cumplimiento de las atribuciones y funciones del personal, cuyo funcionamiento requiere de la utilización de diversos recursos tecnológicos como equipos de cómputo, la red interna de datos, el servicio de internet y los programas de correo electrónico.

- Las cuentas de correo electrónico son propiedad de la Institución y están integradas con el dominio “saludbcs.gob.mx” y “coeprisbcs.gob.mx”.

- La cuenta de correo electrónico asignada a las personas usuarias es personal e intransferible, siendo una herramienta de comunicación oficial para el cumplimiento de sus funciones institucionales, por lo que debe evitarse su uso con propósitos ajenos a estas.

- La solicitud de correo electrónico institucional deberá hacerse a través de ticket en la Mesa de Ayuda para el Instituto, en caso de COEPRIS, referirse a la Unidad de Sistemas de Información.

- Al crear una cuenta de correo electrónico se asignará una contraseña, que será entregada al usuario y deberá cambiarse al menos una vez cada 6 meses.

- El personal usuario es responsable del resguardo, confidencialidad y uso de la cuenta de correo electrónico asignada, así como de la información que genere y transmita por este medio, por ello debe proteger las contraseñas de acceso.

- Cuando la cuenta de correo electrónico no sea utilizada en un periodo mayor de 60 días, se eliminará del sistema.

- Queda prohibido leer la correspondencia electrónica ajena, a menos que se esté específicamente autorizado para hacerlo.

- No está permitido crear, copiar, enviar o reenviar cadenas de mensajes no relacionados con las actividades propias de la Institución, tales como cadenas motivacionales, religiosas, políticas o de superación personal.

- Está prohibido abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, ya que pueden contener virus u otros códigos dañinos.

- Está prohibido que los usuarios compartan las contraseñas de sus cuentas de correo.

- Se debe revisar el correo periódicamente y depurarlo.

- Los usuarios deberán capacitarse y entender los riesgos asociados al uso de correo electrónico.

- Se deben atender los requerimientos hechos por el administrador de la red mediante el correo electrónico.

- Será responsabilidad del usuario realizar respaldo de la información que considere importante con el objetivo de tenerla disponible en caso de presentarse algún fallo en el servicio.

Cumplimiento

El cumplimiento del presente documento tiene como finalidad:

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a los servidores públicos que incurren en responsabilidad administrativa, civil o penal como resultado de su incumplimiento.

- Garantizar que los sistemas de información, infraestructura tecnológica y resguardo de datos, cumplan con las políticas, normas y procedimientos de seguridad.
- Garantizar la existencia de controles que coadyuven al uso adecuado y protección de los bienes informáticos, así como el resguardo y seguridad de la Información.
- Las presentes Políticas podrán ser modificadas o actualizadas, según se determine.

Sanciones

Derivado de la supervisión del cumplimiento de estas políticas informáticas y de la normatividad vigente en materia de tecnologías de la información y comunicaciones; la inobservancia de estas derivará en las siguientes acciones:

- Suspender los servicios de red a los usuarios que se les detecte el uso inapropiado, hasta la aclaración del mismo, o de ser procedente la inhabilitación del servicio.

- Bloquear el servicio de red e internet a aquellos usuarios que resulten afectados por algún virus informático y pongan en riesgo la operación de la red de la Institución, hasta que sean desinfectados totalmente.

- En el caso de Oficina Central, reportar a las áreas correspondientes (Jefe inmediato superior) los casos de incumplimiento a las políticas.

- En las unidades administrativas, el incumplimiento de las políticas informáticas de la Institución será notificado a la administración de la unidad a la cual esté adscrito el usuario, a fin de que esta proceda como corresponda.

Glosario

Administrador: Toda persona(s) responsable(s) por la operación día a día de un sistema de cómputo o recursos de una red de cómputo.

Automatización: Ejecución automática de ciertas tareas con el fin de agilizar el desarrollo de los procesos.

Autorización: Proceso de conceder privilegios a los usuarios.

COEPRIS: Comisión Estatal para la Protección contra Riesgos Sanitarios.

Confidencialidad: Característica de los datos y la información de ser revelados únicamente a personas o entidades autorizadas, en la forma y horarios autorizados.

Contraseña: Conjunto confidencial de caracteres utilizado como mecanismo de autenticación para acceder a cuentas, sistemas, equipos o servicios informáticos.

Correo basura: Correo indeseado.

Correo electrónico: Redacción, envío o recepción de mensajes sobre sistemas de comunicación electrónica.

Correo no solicitado: Correo electrónico en el cual no existe relación previa entre las partes y el destinatario no ha consentido explícitamente en recibir la comunicación.

Correo spam: Correo electrónico no solicitado que se envía a un destinatario específico, sin su consentimiento u aprobación, generalmente en forma masiva y con fines comerciales.

Cortafuegos (firewall): Un sistema (hardware, software o una combinación de los dos) que se instala entre una red privada y una red pública para impedir accesos no autorizados hacia o desde la red privada.

Cuenta de correo: Identificador único con una contraseña o password asociada, que se asigna a un usuario para que pueda utilizar el servicio de correo electrónico.

Datos: Representación de hechos, conceptos o instrucciones en una manera formal, apropiada para comunicación, interpretación o procesamiento manual o automático.

Datos personales: Información que identifica o describe a un individuo.

Deber: Una obligación moral.

Disponibilidad: Característica de los datos, la información y los sistemas de información de estar accesibles en forma oportuna y de la manera requerida.

DOF: Diario Oficial de la Federación.

Equipo de cómputo: Las computadoras, equipos de uso personal y sus periféricos, considerando como equipo de cómputo de escritorio (desktop): el gabinete que contiene la Unidad Central de Proceso “CPU”, el monitor, el teclado, el ratón (mouse) y cualquier otro equipo electrónico que transmita, ingrese o extraiga

información del “CPU” (incluye memoria RAM, tarjetas de video, etc.), y a las computadoras portátiles o “laptop” como la unidad en sí misma.

Hardware: Al conjunto de componentes físicos electrónicos que procesa y/o transmite datos y que forman parte de la infraestructura tecnológica de la Institución.

Información: Es el significado asignado a los datos por medio de convenciones aplicadas a ellos.

Integridad: Característica de los datos y la información de ser y permanecer exactos y completos.

Institución: Secretaría de Salud e Instituto de Servicios de Salud de Baja California Sur.

Licencia: Permiso legal otorgado por un tercero con facultades para ello, para utilizar un producto, generalmente software, a cambio de un pago único o periódico.

Mantenimiento Correctivo: La reparación de equipos que presentan alguna falla en su operación.

Mantenimiento Preventivo: Actividades de revisión y reacondicionamiento de equipos en forma programada, para prevenir fallas en la operación de los mismos.

Mesa de Ayuda: Centro de atención y gestión de incidentes relacionados con el uso de recursos informáticos, que provee un punto de contacto para canalizar los requerimientos de soporte técnico. Su acceso es a través de la página web institucional, correo electrónico a la cuenta soporte@saludbcs.gob.mx o mediante una llamada al número 6121751100 ext. 1095.

Openfire: Servicio de mensajería instantánea de código abierto puesto a disposición para comunicación interna.

Particular: No oficial, no laboral.

Política: Es una declaración formal de las reglas que los usuarios de los recursos tecnológicos y de información de una organización deben acatar.

Privado: Particular y personal de cada uno.

Propietario (a): Área responsable de un sistema de información.

Proceso: Conjunto de instrucciones para el cumplimiento de una etapa especifica señalada.

Recursos Informáticos: Hardware y software (datos e información), incluidos los equipos de cómputo y telecomunicaciones.

Responsabilidad: Cargo u obligación moral de responder por un posible error en una cosa o asunto determinado.

Riesgo: Es una pérdida o daño futuro potencial que puede surgir por alguna acción presente.

Seguridad: Medidas tomadas para reducir el riesgo de: 1) acceso y uso no autorizado; 2) daño o pérdida de los recursos, por algún desastre, error humano, fallo en los sistemas, o acción maliciosa.

Servidor: Computadora no necesariamente multiusuario/multitarea que desempeña una función específica, generalmente en forma dedicada y desatendida. En un servidor no trabajan los usuarios.

Servidor intermediario (Proxy): Es un servidor que actúa como intermediario entre una estación de trabajo de un usuario y el internet, que se instala por seguridad, control administrativo y servicio de caché, disminuyendo el tráfico de internet e incrementando la velocidad de acceso.

Sistema: Término genérico utilizado para hacer referencia a sistema de información.

Sistema de información: Personas, equipos informáticos, software, métodos y procedimientos de operación, utilizados para colectar, almacenar, procesar, recuperar o transmitir datos e información de los usuarios.

Software: Conjunto de componentes o instrucciones lógicas que puede ejecutar una computadora.

Spark: Cliente de mensajería instantánea institucional, mediante el cual se conecta al servidor de Openfire.

Tecnología de la Información: Conjunto de equipos de cómputo y sistemas informáticos que permiten el procesamiento digital de información así como los equipos de comunicaciones de tipo satelital, radio, microonda, fibra óptica, cableado digital que permitan la transmisión de voz, video y datos.

Uso aceptable: Uso adecuado, uso tolerable.

Uso apropiado: Uso correcto.

Uso no aceptable: Uso inadecuado, que no se puede tolerar.

Uso particular: No laboral. Es el uso eventual de los recursos para fines no laborales, no relacionados con la Institución.

Usuario: Término utilizado por brevedad para referirse a usuario autorizado.

Usuario autorizado: Persona que mantiene alguna relación oficial o formal con la Institución, a quien se le ha concedido una debida autorización para acceder a un recurso informático con el propósito de desempeñar sus deberes laborales u otras gestiones relacionadas directamente con los intereses de la Institución.

DOF: Diario Oficial de la Federación.