Políticas para uso de Bienes y Servicios Informáticos

POLÍTICAS PARA USO DE BIENES Y SERVICIOS INFORMÁTICOS

Índice

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

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, que serán de observancia obligatoria en la Administración Pública Federal. Publicado en el DOF el 06 de septiembre de 2021, en el cual señala lo siguiente:

Artículo 54.- 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; así como
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.

Señala en el Artículo 57.- Los servicios institucionales de correo electrónico deberán considerar al menos:

a) La inserción de una leyenda de confidencialidad de la información en los correos institucionales emitidos;
b) El control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;
c) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso;

d) Técnicas de autenticación de correo electrónico que permita al receptor comprobar que un correo electrónico fue enviado y autorizado por la Institución poseedora del dominio;

e) Que el envío por internet se realice con mecanismos de cifrado de la información; así como;

f) Contar con los mecanismos necesarios para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos.

La **Ley General de Responsabilidades Administrativas** señala en su Artículo 7, lo que a continuación se transcribe:

"Los Servidores Públicos observarán en el desempeño de su empleo, cargo o comisión, los principios de disciplina, legalidad, objetividad, profesionalismo, honradez, lealtad, imparcialidad, integridad, rendición de cuentas, eficacia y eficiencia que rigen el servicio público. Para la efectiva aplicación de dichos principios, los Servidores Públicos observarán las siguientes directrices:

I. Actuar conforme a lo que las leyes, reglamentos y demás disposiciones jurídicas les atribuyen a su empleo, cargo o comisión, por lo que deben conocer y cumplir las disposiciones que regulan el ejercicio de sus funciones, facultades y atribuciones;

II. (…)

VI. Administrar los recursos públicos que estén bajo su responsabilidad, sujetándose a los principios de austeridad, eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a los que estén destinados.

Artículo 49.- Incurrirá en Falta administrativa no grave el servidor público cuyos actos u omisiones incumplan o transgredan lo contenido en las obligaciones siguientes:

I. (…)
V. Registrar, integrar, custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos;"

La **Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur**, señala en el artículo 186, lo siguiente:
"Son causa de responsabilidad de los sujetos obligados, por incumplimiento de las obligaciones establecidas en la materia de la presente Ley las siguientes:

I. (…)
IV. 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 servidores públicos o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;.

La **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, señala lo siguiente en el Artículo 31:

"Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño,

pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad."

La **Ley Federal del Derecho de Autor**, señala en el Artículo 103, lo que a continuación se trascribe:

"Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste."

Los diversos artículos referentes a cada legislación antes mencionada en este documento, así como aquellos que no se encuentran descritos en el mismo, siempre que sean aplicables a cada caso y los mismos se encuentren relacionados con el tema que nos ocupa, serán considerados Normatividad vigente y aplicable para poder garantizar el cumplimiento del documento denominado "Políticas para uso de Bienes y Servicios Informáticos".

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.

Responsable	Responsabilidad
	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).
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 cuidarlo y mantenerlo 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 el robo, extravío o daño al equipo asignado, ya sea por accidente, descuido o negligencia; al área correspondiente: 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.

- Es uso indebido utilizar los recursos para fines particulares en horario laboral.

- Toda donación y/o comodato de bienes y servicios informáticos debe ser notificada previamente al área Técnica correspondiente.

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

- 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 en forma compartida, son responsables de éste, del uso que se le dé a la cuenta de correo electrónico y del acceso a internet en su caso.

- 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 leyes de derechos de autor, aplicables a textos, elementos multimedios (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 en forma permanente. También debe de permitir el análisis completo programado de forma mensual. Este

análisis se agenda los últimos días del mes, programados 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 accesar a redes sociales, sitios de descarga de archivos, películas, música, fotos o cualquier otro que atente contra los derechos de autor.

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

- No está permitido utilizar internet para accesar a sitios que sintonizan estaciones de radio y/o televisión, sitios recreativos, deporte, juegos, chistes, redes sociales o sitios de entretenimiento o variedades. Salvo la Unidad de Comunicación Social e Investigadores del área COEPRIS, por las funciones propias de estas áreas.

- 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 sistema de información deberá ser presentada vía oficial por parte del área requirente al área Técnica correspondiente, siendo responsabilidad del área solicitante el 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, deben 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 los niveles de permisos de éstos 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 será supervisado de acuerdo a los estándares nacionales e

internacionales vigentes, deberá contar con memoria técnica y garantía por mínimo 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 o passwords de usuario, serán entregadas vía personal a cada usuario. El manejo seguro de toda contraseña o password es responsabilidad del usuario.

- No se debe prestar las contraseñas o passwords personales.

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

- La contraseña o password deberá ser cambiada por el usuario por lo menos cada 6 meses. La contraseña o password debe ser de 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 área, podrá utilizar la cuenta inicialmente asignada, pero deberá de comunicar 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.

- Se asignará una contraseña o password al momento de crear una cuenta de correo electrónico, misma que se entregará al usuario, la cual se sugiere cambiarla 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 es permitido crear, copiar, enviar o reenviar cadenas de mensajes no relacionados con actividades propias de la Institución, tales como cadenas motivacionales, religiosas, políticas y 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 o passwords 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 información y comunicaciones; la inobservancia de las mismas, derivaran 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 a las políticas informáticas de la Institución será notificada a la Administración de la unidad en la cual esté adscrito el usuario, a fin de que ésta proceda como corresponda.

Glosario

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

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.

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.

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.

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, software (datos e información), incluyendo 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.