POLÍTICAS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE LA "CAJA MUTUAL DE LOS EMPLEADOS DEL MINED"

Descripción breve

Las Políticas de Tecnologías de Información y Comunicaciones a implementarse por la Unidad de Tecnologías de Información, están diseñadas con el fin de garantizar la conservación y el buen uso de los recursos y servicios informáticos con que cuenta la institución.

Elaboró:	Revisó:	Aprobó:
Unidad de Tecnologías de Información	Gerente	Consejo Directivo
Fecha: 07/12/2017	Fecha:	Fecha:
Número de Versión: 1		

CONTROL DE CAMBIOS Y MEJORAS

Una vez aprobado las presentes Políticas de Tecnologías de Información y Comunicaciones podrá ser modificado por el Consejo Directivo.

Al ser aprobadas las Políticas, se procederá a difundirlas en medio físico o electrónico a todo el personal y divulgarlos en la página web de La Caja y otros medios.

TABLA DE CONTENIDO

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

1. INTRODUCCIÓN

La Unidad de Tecnologías de Información identifica la información como un componente indispensable para alcanzar los objetivos definidos por la administración de la institución, razón por la cual es necesario establecer un marco que se asegure que la información manejada, procesada, transportada o almacenada por medio de recursos informáticos esté protegida, de igual forma asegurar la disponibilidad de los servicios y dar continuidad a los procesos. Dadas las cambiantes condiciones y nuevas plataformas de tecnológicas disponibles, la posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado la aparición de nuevas amenazas en las tecnologías de información y comunicaciones.

Esto ha provocado que muchas organizaciones gubernamentales y no gubernamentales, alrededor del mundo, hayan desarrollado documentos y directrices que orientan a las y los usuarios, en el uso adecuado de herramientas tecnológicas, recomendaciones para obtener el mayor provecho de estas, de igual forma evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios que prestan las instituciones a sus clientes.

La seguridad de los servicios y recursos informáticos es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y las/los usuarios. Las políticas de tecnologías de información y comunicaciones, surgen como un lineamiento organizacional para concientizar a cada uno de sus miembros sobre la importancia y sensibilidad de la información, por lo que es necesario controlar servicios críticos que permiten a la institución alcanzar sus objetivos. La implementación de las políticas requiere un alto compromiso del titular, de la administración y demás personal, para obtener mejores resultados.

La masiva utilización de recursos informáticos entre los cuales podemos mencionar: computadores, impresoras, dispositivos de almacenamiento externos, redes de datos, dispositivos móviles, servidores, etc. como medio para almacenar, transferir y procesar información, se ha incrementado desmesuradamente en los últimos años, al grado de convertirse en un elemento esencial para el funcionamiento de la sociedad y de las diferentes empresas e instituciones.

La información y los recursos informáticos, son un activo de altísimo valor, por lo tanto, es necesario proteger, asegurar y administrar la información para garantizar su integridad, confidencialidad y disponibilidad, de conformidad con lo establecido por la Ley. El uso de aplicaciones electrónicas tales

como: correo electrónico, internet, transacciones, firmas y certificados digitales, comunicaciones seguras, servicios remotos, aplicaciones móviles, entre otras, va incrementando según se requieren en la automatización de procesos y manejo de la información. Por tal motivo, las medidas y controles de seguridad deben ser mayores, para evitar fuga de información que proporcionan los clientes externos e internos.

2. DISPOSICIONES GENERALES

Las políticas de tecnologías de información y comunicaciones son un conjunto de normas, reglas, procedimientos y prácticas que regulan la protección y resguardo de la información, con el objetivo de poseer información de calidad. Por medio de la implementación de las mismas, se pretende conservar las características esenciales de la información[1], las cuales se definen a continuación:

a. **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
b. **Integridad:** Es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
c. **Disponibilidad:** Es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

Se han considerado factores tanto accidentales como intencionales, que pueden afectar en determinado momento los recursos informáticos que resguardan la información. De igual es necesario garantizar la conservación y buen uso de los recursos informáticos con que cuenta la institución y la continuidad de los servicios tecnológicos que se proporcionan los empleados.

Las políticas de tecnologías de información y comunicaciones, constituyen los lineamientos que el personal de la institución debe seguir para poder así, hacer buen uso de los servicios y recursos informáticos propiedad de La Caja Mutual de los Empleados del Ministerio de Educación (a partir de ahora "La Caja"). Son un conjunto de compromisos compartidos, que le permiten a la institución, actuar proactivamente ante situaciones que comprometan la integridad de la información, son parte del engranaje del sistema de seguridad que La Caja posee para salvaguardar sus activos y su aplicación es obligatoria, en el uso y acceso a los sistemas de información críticos, componentes de hardware y

[1] Según lo define la **ISO-27001** referente a la Gestión de Seguridad de la Información.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
SAN SALVADOR, C.A.

software, componentes de redes y comunicaciones, así como bases de datos y desarrollo. La implementación de las políticas constituye un proceso continuo y de retroalimentación que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, para lograr la aceptación general, medible en función a los indicadores de disponibilidad de los servicios y sistemas, los niveles de incidencias, amenazas y vulnerabilidades detectadas.

Las políticas por sí solas no constituyen una garantía para la seguridad de la información institucional, ellas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la institución. Ante el incumplimiento de estas políticas, la Jefatura de Tecnologías de Información, remitirá un reporte a Gerencia y Subgerencia, con copia a la Jefatura inmediata superior de la persona involucrada.

3. OBJETIVO

Establecer las normas de regulación para el uso adecuado de los recursos de tecnologías de información y comunicaciones que rigen las gestiones laborales de las y los usuarios, protegiendo la información de los sistemas informáticos, asegurando la disponibilidad e integridad de los servicios y recursos del ambiente tecnológico de La Caja; garantizando además la eficiente administración de las herramientas tecnológicas.

4. ALCANCE

Las presentes políticas son de cumplimiento obligatorio para los funcionarios y empleados de La Caja, así como aquellas que, sin tener un vínculo laboral, se les permita el acceso al hardware y software propiedad de La Caja. Incorporan responsabilidad administrativa e incluso civil o penal para aquella persona que incumpla las normativas de seguridad informática establecidas en este documento, de

conformidad con el régimen jurídico vigente, avalado por el "Art. 1"[2] de la "Ley especial contra los delitos informáticos y conexos"; y demás artículos expresados en dicha Ley que respalden las presentes políticas.

Por lo anterior, la Unidad de Tecnologías de Información deberá enviar vía correo electrónico, una copia del presente documento a cada persona, funcionario, empleado, personal contratado por servicios profesionales y contratistas de La Caja, que deberán conocer y cumplir los lineamientos establecidos en el mismo. Se consideran violaciones graves el robo, daño, divulgación de información confidencial de La Caja, el uso inadecuado de recursos y servicios informáticos, así como el daño intencional de estos, o que se le declare culpable de un delito informático cometido, tomando de referencia el marco legal vigente.

5. NORMATIVAS APLICABLES RELACIONADAS

El presente documento de "Políticas de Tecnologías de Información y Comunicaciones de la Caja Mutual de los Trabajadores del Ministerios de Educación", está enmarcado en las disposiciones legales vigentes que le son aplicables, tales como:

- **"Reglamento para el uso y control de las tecnologías de información y comunicación en las entidades del sector público".** Según Decreto Nº 24 de La Corte de Cuentas de la República de El Salvador, publicado en el Diario Oficial Tomo Nº 404, de fecha martes 8 de julio de 2014.
- **"Ley especial contra los delitos informáticos y conexos".** Según Decreto Nº 260 de La Asamblea Legislativa de la República de El Salvador, publicado en el Diario Oficial Tomo Nº 410, de fecha viernes 26 de febrero de 2016.
- **"Ley especial para la intervención de las telecomunicaciones".** Según Decreto Nº 285 de La Asamblea Legislativa de la República de El Salvador, publicado en el Diario Oficial Tomo Nº 386, de fecha lunes 15 de marzo de 2010.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

[2] **Art. 1.-** La presente Ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.

6. RESPONSABILIDADES

Unidad de Tecnologías de Información: Que en adelante se nombra UTI, conformada por el conjunto de profesionales de la rama de Tecnologías de Información, responsables de dar soporte a las y los usuarios, cubrir los requerimientos tecnológicos de La Caja; así como hacer cumplir las políticas plasmadas en este documento y mitigar posibles afectaciones contra la seguridad de la información.

Jefatura de Tecnologías de Información: Es la responsable de dirigir y administrar eficiente y eficazmente al personal de la Unidad, así como de los procesos allí generados. Además de velar por la automatización de los procesos administrativos. Durante el desarrollo del documento se hará alusión a la/el Jefe de UTI o Jefatura de UTI.

Usuarias/Usuarios: Son las personas, empleadas o empleados y funcionarias o funcionarios distribuidos en la estructura jerárquica de La Caja, que utilizan recursos de tecnología de información, responsables de cumplir con las políticas referidas y del buen uso y cuidado de los equipos, servicios o recursos informáticos proporcionados por la institución para el desempeño de sus funciones.

Administración de La Caja: Integrada por Presidente, Gerente y Sub-Gerente son los responsables de velar por el cumplimiento de las políticas de tecnologías de información y comunicaciones.

7. DEFINICIONES[3]

Amenaza. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Ataque cibernético. Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.

Ataque de negación de servicio (DDoS). Es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos.

Automatización. Es un sistema donde se trasfieren tareas realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos, que sirven para estandarizar los procesos de trabajo.

Buzón. También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la institución.

[3] **Fuente:** Definiciones proporcionadas en las Leyes y normativas aplicables consultadas, así como consultas vía web a diferentes diccionarios informáticos.

Canales electrónicos. Son medios de transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y demás relacionadas con las tecnologías de información y la comunicación.

Ciclo de vida del desarrollo de sistemas. Proceso que se sigue para construir, entregar y hacer evolucionar el sistema de información, desde la concepción de una idea hasta la entrega y retiro del sistema.

Cliente de correo electrónico. Programa informático para la gestión individual de cuentas de correo electrónico, envío y recepción de información.

Computadora. Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Contingencia. Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de diferentes herramientas informáticas/dispositivos, necesarias para el funcionamiento óptimo institucional.

Contraseña o password. Conjunto de números, letras y caracteres, utilizados para reservar el acceso a las y los usuarios que disponen de esta contraseña.

Correo electrónico. También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red.

Cuentas de correo. Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico.

Descargar o bajar (Download). Transferencia de información desde Internet a una computadora.

Dispositivo. Cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnologías de la Información y la Comunicación.

Electricidad estática. Se presenta cuando no existe ninguna fuerza externa (voltaje) que impulse a los electrones o si estos no tienen un camino para regresar y completar el circuito, la corriente eléctrica "no circula".

FTP. Es un protocolo de red para la transferencia de archivos entre sistemas interconectados o enlazados a Internet, basado en la arquitectura cliente-servidor.

Hacker. Persona dedicada a lograr un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red con el objeto de alterar en forma nociva su funcionamiento.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet. Red privada dentro de una institución, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

LAN. (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Log. Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

JEFE DE TECNOLOGÍAS DE INFORMACIÓN

Malware. Es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Mantenimiento Preventivo. Servicio con la finalidad el prevenir o minimizar la posibilidad de fallas en los equipos informáticos.

Mantenimiento Correctivo. Servicio de atención ante una avería o falla en cualquier equipo informático.

Megabyte (MB). Es una cantidad de datos informáticos. Es bien un millón de bytes ó 1.048.576 bytes.

Medio de almacenamiento. Es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin ayuda de cualquier otro medio idóneo.

Phishing. Es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Proveedor de servicios. Persona natural o jurídica que ofrece uno o más servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos.

Redes Sociales. Estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información.

Servidor de correo. Dispositivo especializado en la gestión del tráfico de correo electrónico. Su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben las y los usuarios.

S.O. (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Seguridad Informática. Es una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos informáticos en una organización. Medidas y controles que aseguren la confiabilidad, integridad y disponibilidad de los activos incluyendo hardware, software, firmware y la información que es procesada, almacenada y comunicada.

Sistemas de Información. Se entiende como el conjunto de tecnologías, procesos, aplicaciones de negocios y software disponibles para las personas dentro de una organización.

Software. Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Soporte Técnico. Servicios que proporciona asistencia con el hardware o software de una computadora, o algún otro dispositivo electrónico, para ayudar a resolver los problemas que puedan presentárseles a las y los usuarios, mientras hacen uso de servicios, programas o dispositivos.

SPAM. Es la denominación del correo electrónico no solicitado que recibe una persona. Dichos mensajes, también llamados correo no deseado o correo basura, suelen ser publicidades de toda clase de productos y servicios.

Tecnologías de Información y Comunicación. Conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento,

control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de vos, imágenes y datos.

Telecomunicaciones: Cualquier tipo de transmisión, emisión, recepción de signos, símbolos, señales escritas, imágenes, correos electrónicos, sonidos o información de cualquier naturaleza por hilos, radioelectricidad, medios ópticos u otro sistema electromagnético, quedando comprendidas las realizadas por medio de telefonía, radiocomunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar.

UPS (Sistema de alimentación ininterrumpida). Dispositivo que puede proporcionar energía eléctrica por un tiempo limitado y durante una interrupción eléctrica a todos los dispositivos que tenga conectados.

URL. Se trata de la secuencia de caracteres que siguen un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados.

Virus. Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas, causando serios problemas a los sistemas infectados.

Vulnerabilidad. Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. POLÍTICAS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Las políticas de tecnología de información y comunicaciones, se han elaborado en función al uso de recursos y servicios informáticos, para establecer una administración y control adecuado de los mismos, como se presenta a continuación:

a) Política de uso de cuentas de usuario
b) Política de uso del servicio de internet
c) Política de uso de portal web, canales electrónicos y redes sociales
d) Política de uso de correo electrónico
e) Política de control de red interna
f) Política de instalación de hardware y licencias de software
g) Política de uso de equipo informático
h) Política de gestión de copias de seguridad o respaldo de información
i) Política de uso de impresores y periféricos
j) Política de ingreso al área de servidores
k) Política de mantenimiento preventivo y correctivo de equipos informáticos
l) Política de desarrollo y actualizaciones de sistemas informáticos
m) Política de asignación, uso y control de teléfono móvil institucional

Políticas Generales:

a) La Unidad de Tecnologías de Información, deberá estar ubicada en un nivel jerárquico que le permita ejercer la gobernabilidad e independencia funcional dentro de La Caja[4].
b) La gestión de las tecnologías de información y comunicaciones, es responsabilidad de la administración general y de la UTI, la cual debe contar con los recursos adecuados, que garanticen el cumplimiento de los objetivos institucionales[5], según el Plan Estratégico vigente.
c) La Jefatura de la UTI deberá proponer a la máxima autoridad de La Caja, las necesidades y requerimientos tecnológicos de las dependencias, proyectar las mejoras en las tecnologías de información y comunicaciones, considerando los costos, viabilidad, capacidad técnica,

[4] Art. 3 del Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.
[5] Art. 9 del Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

instalaciones, riesgos tecnológicos, vida útil y tasas de crecimiento de la infraestructura tecnológica.

d) Todos los usuarios y usuarias de la Caja deberán conocer las políticas aquí establecidas y regirse en su actuar por las normativas descritas, por tanto, bajo ninguna circunstancia, deben utilizar los recursos informáticos para realizar actividades contrarias a las definidas.

e) La UTI, es la responsable de concienciar a las usuarias y usuarios, sobre la obligación de conocer y aplicar las presentes normativas, para lograr un cambio favorable en la cultura organizacional.

8.1 Política de uso de cuentas de usuario

Se entenderá por cuenta de usuario la que constituye la principal vía de acceso a los recursos informáticos, que así lo requieran; permitiendo aislarlo del entorno, asignándole privilegios en el uso, impidiendo perdidas de información en los sistemas o los datos de otros, y permitiendo a su vez que pueda personalizar su entorno sin afectar configuraciones del propietario de la cuenta.

Las y los usuarios que accedan a sistemas de comunicación o redes deben de poseer una sola cuenta, asignada a un equipo, en caso de que dos personas tengan acceso a un mismo equipo, se podrá asignar una segunda cuenta, según análisis de los puestos de trabajo y funciones, realizado por la UTI. Esto permite realizar seguimientos y controles, evitando modificar las configuraciones, previniendo la pérdida o fuga de información del usuario, accesos al buzón de correo no autorizados o inicios de sesión no autorizados.

Asignación y uso de cuentas de usuario:

a) La asignación de cuentas y cambio de privilegios o el restablecimiento de clave de inicio de sesión en las computadoras, deberá ser remitida por las Jefaturas de la Unidad o Área, a la que pertenece la o el usuario, esta se realizará por ingreso de ticket en Sistema de Soporte o por correo electrónico y será autorizada por la Jefatura de la UTI.

b) Cuando la o el usuario olvide o bloquee su contraseña, deberá acudir a la UTI para que se le restablezca provisionalmente y se habilite el cambio al iniciar sesión en el equipo automáticamente, para que pueda ingresar una nueva.

JEFE DE TECNOLOGÍAS DE INFORMACIÓN

c) La o el usuario cambiará la contraseña inicialmente asignada, la primera vez que ingrese a la red, correo electrónico y sistemas de información.

d) La contraseña temporal asignada, sólo debe suministrarse una vez identificado la o el usuario. Para prevenir los ataques contra los intentos de adivinar la clave, la cuenta será desactivada después tres (3) intentos erróneos consecutivos.

e) La contraseña deberá contener una longitud mínima de 10 caracteres alfanuméricos, el primer carácter será letra en mayúscula.

f) La contraseña de acceso a la red por seguridad se cambiarán cada 60 días calendario.

g) Las contraseñas no deben mantenerse de forma legible en cualquier medio impreso o dejarla en un lugar donde personas no autorizadas puedan tener acceso a los datos.

h) Cuando la o el usuario recibe una cuenta, debe firmar un documento, elaborado por la UTI, donde declara conocer las políticas y procedimientos de seguridad informática y acepta sus responsabilidades con relación al uso de esa cuenta.

i) Las y los usuarios no deben proporcionar el nombre de la cuenta ni contraseña, a otras personas, a menos que estén debidamente autorizados.

j) Las y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a las y los administradores del sistema.

k) Las y los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (ID).

l) La Unidad de Desarrollo Humano debe reportar a la UTI, al personal que cesa sus actividades y solicitar la desactivación de su cuenta esto en un máximo de dos días hábiles posterior a la fecha del cese de las actividades.

m) Los privilegios especiales de borrar o depurar los archivos de otras y otros usuarios, sólo se otorgan al personal de la UTI.

n) No se otorgará cuentas a técnicos de mantenimiento externos o personas que no tienen nada que ver con la UTI, ni permitir su acceso remoto con ningún tipo de software, a menos que la Jefatura de la UTI determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (Ejemplo: el mantenimiento remoto).

o) No se crearán cuentas anónimas o de invitado.

p) Se asignarán los inicios de sesión en las computadoras según la necesidad que se presente, las y los usuarios no podrán acceder a otros equipos con sus credencias sin la previa autorización. De ser necesario deberá solicitar el cambio a la UTI por ingreso de ticket en Sistema de Soporte o por correo electrónico.

q) Los horarios de uso de los equipos estarán delimitados para los días hábiles comprendidos de lunes a viernes de las 6:00 am a 8:00 pm, dando este margen para el correcto funcionamiento de las actividades institucionales, si la o el empleado necesita hacer uso del equipo asignado a su persona en horario fuera del establecido deberá solicitar la modificación temporal, indicando el periodo de tiempo que necesita para la finalización de las actividades, a la UTI por ingreso de ticket en Sistema de Soporte o por correo electrónico, con el visto bueno de la o el Jefe inmediato.

8.2 Política de uso del servicio de internet

El propósito de esta política es establecer normas que aseguren el buen uso del servicio de navegación por Internet, como una herramienta que permita mejorar el desempeño del trabajo del personal y facilite el logro de los objetivos de la Institución, su uso estará habilitado en forma extraordinaria y de manera controlada, para evitar los riesgos que representa, como por ejemplo: malware, spam, ataques cibernéticos que podrían dañar las computadoras y/o sistemas, representando pérdidas de información o ataques de denegación de servicios que afectarían la red de datos local. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas, valiéndose de los recursos que les provee la conexión a internet para obtener accesos no autorizados.

Por tanto, las conexiones a internet deberán ser previamente autorizadas y serán protegidas por medio de dispositivos de seguridad, los cuales estarán ubicados entre la red privada local y el proveedor de servicios de internet, estos dispositivos controlarán las entradas y salidas a internet de los equipos autorizados para navegación.

Las políticas se aplicarán en función de resguardar la información, la UTI está facultada para realizar monitoreo constante, por lo que la y el usuario deberá tener a consideración lo siguiente:

a) El servicio de internet es gestionado por la UTI en función al ancho de banda requerido, considerando el número de usuarias y usuarios conectados y los servicios habilitados sobre el enlace.

JEFE DE TECNOLOGÍAS DE INFORMACIÓN

b) Se habilitará servicio de internet a las y los usuarios con niveles de acceso y restricciones definidos, con autorización de la o el Jefe inmediato justificando su uso, la Jefatura de la UTI avalará la solicitud, la cual se recibirá por medio de correo electrónico o por ingreso de ticket al Sistema de Soporte.

c) Las configuraciones en la computadora, navegador y dispositivos informáticos para acceso a internet por medio de la red cableada o inalámbricas, son de exclusiva responsabilidad de la UTI, estas acciones están orientadas a asegurar el ancho de banda necesario para el uso del internet y de los servicios que brinda la red y que son de interés de la Institución.

d) El acceso a internet en las computadoras de los empleados y empleadas, será establecido en horario de 6:00 am a 8:00 pm, de lunes a viernes, es de uso para fines laborales no personal, con el propósito de no saturar el ancho de banda y así poder hacer buen uso del servicio.

e) El acceso a la red inalámbrica interna es limitado para uso en actividades laborales. Se tendrá restringido el acceso a redes inalámbricas en Salas de Reuniones para uso exclusivo de computadoras que pertenezcan a La Caja, no se podrán agregar dispositivos móviles o similares. De requerirse acceso a personas externas a la institución será autorizado por la Jefatura de la UTI.

f) Las restricciones de acceso a páginas web serán controladas por la clasificación de su contenido definidas de forma predeterminada por el dispositivo de seguridad perimetral firewall, las categorías se definen de la siguiente manera:

- Potencialmente riesgosas: abuso de drogas/estupefacientes, abuso de niño, discriminación, evasiones de proxies, grupos extremistas, hacking, ilegal o no ético, plagio de material propietario, violencia explícita.
- Contenido adulto/maduro: aborto, alcohol, pornografía, apuestas, venta de armas, otros materiales de contenido similar.
- Alto consumidor de ancho de banda: compartición de archivos punto a punto, descargas de programas gratuitos, intercambio de archivos y almacenamiento, radio y TV por internet, telefonía internet, transmisión de medias y descargas.
- Violación de la seguridad: phishing, sitios web maliciosos, URL de mensajes no solicitados, Spam.
- Contenidos de interés general – personal: anuncios, búsqueda de empleo, correo electrónico basado en la web, deportes, educación, grupos de noticias y foros de mensajes, juegos,

entretenimiento, contenido dinámico, contenido sin sentido, medicina, mensajería instantánea, noticias y medios, pláticas por web, redes sociales, salud y bienestar, sociedad y estilos de vida, religiones mundiales, sitios web personales y blogs, tarjetas postales digitales, viajes.

- Contenidos de interés general – negocio: aplicaciones basadas de web, banca y finanzas, hospedaje web, información y seguridad en cómputo, negocios, organizaciones legales y de gobierno, organizaciones generales, sitios web seguros, tecnologías de información.

g) Se prohíbe la descarga de programas, demos, tutoriales, material multimedia, documentos, archivos comprimidos o archivos adjuntos en correos electrónicos de cuentas personales, que no sean de apoyo para el desarrollo de las tareas diarias de cada usuaria o usuario, verificando que las fuentes sean confiables, de remitentes conocidos y sitios web certificados.

h) Se tendrá acceso solo a la información necesaria acorde al desarrollo de sus actividades.

i) Queda restringido el acceso a sitios de contenido multimedia, se tomarán a consideración el uso racional de estos recursos para fines laborales; el uso de sitios de descarga o distribución punto a punto quedará restringido, debido al alto consumo de recursos de Internet/Intranet que utilizan y las vulnerabilidades que representan.

j) No se deberá utilizar aplicaciones web para realizar llamadas internacionales o video conferencias de tipo personal. Únicamente y previa autorización, podrán realizar video conferencias, en caso sus funciones y necesidades lo requirieran.

k) La UTI tiene la facultad de monitorear la actividad y uso servicio de internet por persona usuaria e informar a Gerencia sobre todo acceso a un sitio de contenido NO apropiado, para responsabilizarla por cualquier eventual contagio, del equipo informático asignado, red institucional o desperfecto ocasionado por la sola visita a este tipo de sitios.

l) Es de exclusiva responsabilidad de la UTI planificar periódicamente la revisión de las configuraciones del PC y navegador, siempre orientado a asegurar el ancho de banda para las aplicaciones y uso de interés de La Caja, realizando la revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas.

m) En caso se determine que alguna de las páginas previamente restringidas sea requerida para el desempeño de funciones de algún usuario esta será habilitada únicamente con el consentimiento y solicitud de su Jefe directo, con el visto bueno de la UTI.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

n) La UTI, velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución. La UTI no se hará responsable por incidentes producidos por el NO cumplimiento de estas políticas.

8.3 Política de uso de portal web, canales electrónicos y redes sociales

El objetivo de esta política es definir la metodología de difusión, publicación y promoción de contenido del portal, canales web y redes sociales oficiales de La Caja, que están a disposición pública.

La Administración General de La Caja y la UTI, reconoce que el portal web y los diferentes canales electrónicos y redes sociales, son medios tecnológicos, que facilitan la comunicación, la difusión de información, la vinculación con las actividades y eventos institucionales, facilitando la promoción de los productos y servicios que La Caja proporciona a la población usuaria en general.

La institución está comprometida a proteger la seguridad de los contenidos, la confidencialidad y los derechos de autor. Por este motivo se dará estricto cumplimiento a toda la legislación pertinente.

a) La Jefatura de Participación Ciudadana, Publicidad y Comunicaciones, deberá de mantener la calidad y actualización de la información publicada en el portal web, los canales electrónicos y redes sociales.

b) El portal web, los canales electrónicos y redes sociales reconocidos oficialmente por la Administración General de La Caja, publicados bajo la marca en el Portal de Transparencia, administrado por la Oficina de Información y Respuesta son:

   - Portal Web: **www.cajamined.gob.sv**.
   - Canales electrónicos y redes sociales: En Facebook **www.facebook.com/Cajamined**, Flickr para publicación de fotos bajo el nombre **"Caja Mutual"**, Twitter **www.twitter.com/cajamined** y YouTube **www.youtube.com/cajamined**.

   Otros sitios registrados bajo la marca "Caja Mutual" o "Caja Mined" no serán reconocidos como medios informativos autorizados.

c) La Jefatura de Participación Ciudadana, Publicidad y Comunicaciones deberá notificar a la Gerencia, Subgerencia o a las instancias que deban ser informadas, sobre los asuntos relevantes que sean tratados a través del portal web, redes sociales o los canales electrónicos oficiales.

d) Los empleados de La Caja deberán abstenerse de utilizar información publicada en medios informativos autorizados de La Caja o lo concerniente a las actividades institucionales en medio no autorizados, en sus redes sociales o canales electrónicos.

e) La UTI deberá contar con los mecanismos y herramientas necesarias para implementar controles enfocados en la estructura del portal web, para resguardar la integridad, disponibilidad y confidencialidad de la información que se transmite a través del mismo.

f) La UTI coordinará con la Jefatura de Participación Ciudadana, Publicidad y Comunicaciones, la implementación de mejora continua en los procesos de soporte de los servicios que se proporcionan por medio de los canales electrónicos.

g) Los requerimientos mínimos de diseño de la plataforma web, canales electrónicos y redes sociales, deberán cumplir con el estándar gubernamental definido en las "Políticas y lineamientos para uso de medios sociales de instituciones de Gobierno", que contiene la guía de los lineamientos y políticas para la gestión de información y mensajes difundidos a través de los medios sociales de las instituciones públicas. El proceso de estandarización es monitoreado y evaluado por la "Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador"[6].

8.4 Política de uso de correo electrónico

El correo electrónico institucional, de aquí en adelante el correo, se debe utilizar de forma responsable. Su propósito es servir como herramienta para agilizar las comunicaciones oficiales, internas y externas, que apoyen la gestión institucional de La Caja; este debe ser utilizado de forma eficiente, eficaz, ética y de acuerdo con la ley. Es importante aclarar que cada unidad administrativa decidirá aquellos asuntos que deberán tratarse por canales tradicionales de comunicación. La información transmitida mediante el servicio de correo electrónico institucional es responsabilidad única y exclusiva de la o del usuario que la genera. El contenido de los mensajes por correo electrónico no gozará de validez jurídica, en tanto no correspondan formalmente a un procedimiento administrativo previsto en cualquier normativa aplicable a la institución. Se exceptúan los correos remitidos por servidores públicos a particulares en cumplimiento de una habilitación legal, según lo argumenta el "Art. 85"[7] de Ley de Acceso a la Información Pública.

---

[6] Dirección de Medios Digitales y Redes Sociales Secretaría de Gobernabilidad y Comunicaciones, correspondiente a Casa Presidencial de la República de El Salvador.

[7] **Art. 85.-** El Instituto podrá adoptar las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales en cualquier momento del procedimiento, mediante resolución motivada. En particular, podrá: a. notificarse al superior jerárquico del infractor de la existencia de posibles conductas infractoras y de la incoación del recurso ante el Instituto. b. solicitar al titular de la entidad la adopción de medidas especiales de resguardo y copia de seguridad de la información de que se trate. c. solicitar una copia de la información objeto de la apelación excepto si es de naturaleza reservada, la copia será resguardada de manera confidencial por el Instituto y devuelta al final del incidente de apelación. Estas medidas se tomarán con resguardo de los derechos de los particulares a la protección de sus datos personales cuando éstos pudieran ser afectados. Se respetará, en todo caso, el principio de proporcionalidad de la medida con los objetivos que se pretendan alcanzar en cada supuesto. En ningún caso podrá ordenarse como medida cautelar el secuestro o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

El correo se encuentra dentro de la esfera de protección constitucional que procede del principio de inviolabilidad de la correspondencia detallado en el "Art. 24"[8] de la Constitución de la República de El Salvador y respaldado por el "Art. 1"[9] de la Ley Especial para la Intervención de las Telecomunicaciones[10] Por tanto, para su uso adecuado la persona usuaria deberá tener en cuenta los siguientes lineamientos:

a) Es responsabilidad de la UTI la administración de las cuentas de correo, solicitadas por las Jefaturas de las diferentes unidades de la institución.
b) La cuenta de correo electrónico institucional es personal, inviolable e intransferible. Si una cuenta no presenta ningún tipo de transacción en un período de 30 días, esta se bloqueará automáticamente; y en 90 días se eliminará totalmente del servidor.
c) Únicamente la UTI, está facultada para configurar y habilitar cuentas de correo electrónico en las computadoras o dispositivos móviles institucionales, para la realización de sus actividades laborales. No se asignará cuenta de correo en dispositivos de terceras personas.
d) El correo deberá ser utilizado como una herramienta de trabajo, está prohibido su uso para:
   - Enviar y recibir asuntos personales, comerciales, deportivos, humorísticos, políticos, religiosos, entre otros.
   - Suscribirse a redes sociales, canales de noticias, boletines, publicidad y correo diferentes a los fines de la institución.
   - Participar en la propagación de correos encadenados, en esquemas piramidales o similares.
   - Realizar comunicaciones de contenido pornográfico, ilícito o degradante, de contenidos impropios y/o lesivos a la moral.
e) No se deberá enviar archivos de gran tamaño, que supere los 8 megabytes de tamaño. Para transmisión de archivos entre cuentas de correo internos, que superen el tamaño definido se deberá solicitar la creación de carpetas compartidas entre las unidades o el medio que defina la UTI, según solicitud de la Jefatura de la unidad solicitante.

[8] **Art. 24.-** La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas.
[9] **Art. 1.-** Se garantiza el secreto de las telecomunicaciones y el derecho a la intimidad. De manera excepcional podrá autorizarse judicialmente, de forma escrita y motivada, la intervención temporal de cualquier tipo de telecomunicaciones, preservándose en todo caso el secreto de la información privada que no guarde relación con la investigación o el proceso penal. La información proveniente de una intervención ilegal carecerá de valor.
[10] **Telecomunicaciones.-** Cualquier tipo de transmisión, emisión, recepción de signos, símbolos, señales escritas, imágenes, correos electrónicos, sonidos o información de cualquier naturaleza por hilos, radioelectricidad, medios ópticos u otro sistema electromagnético, quedando comprendidas las realizadas por medio de telefonía, radiocomunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar.

f) El uso de la cuenta y/o buzón del correo electrónico institucional es exclusivo para la o el usuario que se le asigne, no deberá ser expuesta a terceras personas.

g) Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos contenidos en correo de origen desconocido, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, entre otros) lo que puede conllevar al robo de información institucional, por lo que se deberá reportar inmediatamente a la UTI, para verificar el contenido y tomar las medidas necesarias de seguridad.

h) Se deben borrar los mensajes catalogados como spam o correo basura sin leerlos de forma periódica. En caso de duda, se deberá consultar a la UTI. Se deben eliminar permanentemente los mensajes innecesarios, así como de organizar los mensajes que desea conservar, agrupándolos según la o el usuario considere conveniente.

i) Al requerir contestar un correo de difusión masiva, las y los usuarios deben evitar realizarlos con la opción "Responder a todos" en caso que el mensaje contenga información de uso privado o no sea requerida por las y los receptores.

j) El acceso a las cuentas de correo personales deberá ser moderado durante la jornada laboral. A excepción cuando el correo institucional tenga fallas técnicas y se requiera recibir o enviar correos, se podrá realizar por el correo personal de manera temporal, mientras se restablece el correo institucional.

k) La o el usuario es responsable de establecer una contraseña para el uso del correo asignado, esta contraseña deberá ser resguarda para que no pueda ser utilizada por otras personas.

l) Cuando la o el usuario deje de usar su estación de trabajo deberá cerrar el software de correo electrónico, para evitar que otra persona acceda a la misma.

m) Los usuarios que tienen asignada una cuenta de correo, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje o conectarse al correo con la mayor frecuencia posible para leer sus mensajes.

n) La o el usuario es responsable de la redacción y contenido de los mensajes que transmita. Es de carácter obligatorio el cumplimiento de las siguientes indicaciones antes de realizar el envío de correos electrónicos:

   - Verificar el destinatario y el contenido del mensaje antes de enviarlo;

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

- Al enviar un archivo adjunto se debe comprimir - siempre que sea posible - e indicar en el asunto del mensaje el contenido de dicho archivo;
- Usar la firma automática institucional asignada por la Jefatura de Participación Ciudadana, Publicidad y Comunicaciones;
- Las listas de distribución de correo solo deberán usarse para mensajes relacionados con la finalidad de las mismas;
- Los usuarios consultarán con la UTI las indicaciones de uso de las listas de distribución.

o) Se deberá evitar el uso de las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, para no afectar el tráfico de la red de datos.

o) En ningún caso recibir, ni compartir información o archivos adjuntos, proveniente de remitentes desconocidos o ajenos a la institución, para evitar el ingreso de virus al equipo y poner en riesgo la información contenida en el equipo.

8.5 Política de control de red interna

Para resguardar la información que se transfiere en la red de datos local, se requiere establecer parámetros de seguridad que permitan la disponibilidad de los servicios, recursos locales o los proporcionados por proveedores externos, definiéndose los siguientes:

a) Los equipos y dispositivos informáticos institucionales, tendrán acceso a los recursos y servicios de la red, tales como: impresoras, correo electrónico, carpetas compartidas, internet, etc. a través de cuentas de dominio administradas por la UTI.

b) Se incorporan nuevos equipos, servicios y recursos informáticos a la red interna, por requerimiento de las Jefaturas de las diferentes áreas o según el requerimiento de la UTI para mejora de procesos o modernización de la infraestructura tecnológica, será ejecutado por la UTI sujeto a factibilidad técnica y previa autorización de Gerencia.

c) Se proporcionará acceso a carpetas locales, FTP, correo electrónico y demás recursos de red únicamente a equipos propiedad de La Caja y configurados por la UTI.

d) Los servicios actuales para compartir archivos en la red establecidos y administrados por la UTI son: carpeta compartida CAJA-PUBLIC, FTP-AGENCIAS y OWNCLOUD.

- CAJA-PUBLIC: Es una carpeta compartida dentro de la red interna para el personal de La Caja, solo de uso laboral (compartir y almacenar información solo pertinente a sus tareas), no para almacenar cosas personales, con un máximo de 250 megabytes de almacenamiento en cada subcarpeta, la información almacenada en dichas carpetas se vaciará cada día a las 8:00 pm para así liberar espacio en disco evitando que este se mantenga lleno de archivos innecesarios, tomando en cuenta lo anterior cada persona usuaria deberá asegurar de almacenar la información compartida en sus equipos.

  No está permitido almacenar en el recurso CAJA-PUBLIC archivos de música, imágenes, videos, etc. que no sean institucionales. La estructura de la carpeta compartida CAJA-PUBLIC está constituida por diversas subcarpetas así: Administración, Afiliación, Consejo Directivo, Financiera, Servicios Administrativos, dentro de la cual están las carpetas nombradas por cada usuario.

- FTP-AGENCIA: Es un servicio administrado por la UTI, para compartir archivos desde las agencias departamentales a usuarios que se requieran en la oficina central, a través del cliente FileZilla que incorpora el protocolo de transferencia de archivo.
- OWNCLOUD: Es un servidor con los recursos necesarios para compartir archivos, está constituido para un directorio de carpetas distribuido por unidades y carpetas de usuarios. Este servicio será administrado por la UTI y configurado en cada equipo según el uso requerido.

e) La UTI deberá restringir el uso de herramientas para compartir archivos entre áreas, que no sean las autorizadas por la Unidad. Los usuarios no están autorizados para configurar unidades de red o implementar herramientas de software descentralizado de las que utiliza la UTI para compartir archivos.

f) La UTI es la responsable de definir los procesos y definir las aplicaciones de software o mecanismos para compartir información entre áreas, verificando su funcionamiento e implementando medidas de seguridad necesarias para su uso.

g) Queda prohibido eliminar archivos o carpetas de los recursos compartidos, de igual forma trasladar archivos o carpetas personales a los recursos compartidos.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

8.6 Política de instalación de hardware y licencias de software

Todo nuevo recurso para el procesamiento de información, hardware y software, deber ser previamente evaluado para su adquisición y contar con el visto bueno de la Jefatura de la UTI, para garantizar que cumpla con los estándares definidos y su compatibilidad con los componentes de la infraestructura existente. La baja de activos de hardware y software deberá ser registrada y reportada a la Unidad de Logística y Activos para su respectivo descargo de inventario.

Licenciamiento de Software: Solo el personal de la UTI, está autorizado para instalar, modificar, desinstalar y actualizar el software en la computadora asignada. Cuando se necesite algún programa específico para desarrollar una actividad laboral, se deberá comunicar a la Jefatura de la UTI para su autorización. En todo caso se deberá considerar las siguientes normativas:

a) Las licencias o paquetes de software propiedad de la Caja, serán adquiridos solo para fines laborales, por tanto, se prohíbe su instalación en equipos que no pertenezcan a la institución.
b) No se podrá instalar software ilegal o protegido por derechos de autor, sin la respectiva licencia en los equipos computacionales que estén inventariados, con la excepción de licencias que permitan su uso y distribución libre. Por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.
c) No se hará entrega de medios físicos o números de serie de licenciamiento a las y los usuarios que utilicen la licencia, por tratarse de información delicada y confidencial que tiene por objeto proteger los planes de licenciamientos y compromisos legales adquiridos por la institución.
d) La UTI realizará auditorías periódicas de software instalados en los equipos, para verificar software no autorizado y sin justificación de uso, en caso de detectarse se procederá a desinstalarlo. Se realizará informe de la situación detectada en el proceso para informar, a la Jefatura de la Unidad auditada y a la Jefatura de la UTI.
e) Los requerimientos de instalación de software que no cuenten con una licencia valida, deberán ser canalizados formalmente a través del Jefe de Unidad, quien deberá escalar y evaluar el requerimiento junto a la Jefatura de la UTI, para analizar si existen alternativas de software libre, si es posible asignar una licencia disponible, o se gestiona la compra.
f) El contrato corporativo de licenciamiento Microsoft, solo tiene cobertura para equipos que hayan sido adquirido e inventariado por la institución.

g) Todos los equipos contarán con una instalación de software básico correspondiente a funciones administrativas como: sistema operativo, Microsoft Office, Antivirus y utilidades de uso libre o con licencia, según sea el requerimiento del usuario.

h) En caso de que las Unidades utilicen software de terceros, que requieran mantenimientos o modificaciones, será la o el Jefe de la Unidad requirente el responsable o en su efecto el Administrador de Contrato, los encargados de solicitar la adquisición en la contratación de mantenimientos anual, la UTI no se hace responsable de software de tercero, ni de la caducidad de licencias de software que este fuera del período asignado.

Instalación de Hardware: Las y los usuarios no están autorizados a realizar cambios que alteren el funcionamiento de las computadoras, periféricos demás componentes informáticos asignados.

a) La UTI es la responsable de instalar los equipos informáticos, en los puestos de trabajo según se defina.

b) Para realizar el traslado o mover los equipos, la o el Jefe de la Unidad requirente deberá solicitarlo por correo electrónico a la Jefatura de la UTI para su autorización, el proceso será realizado por la UTI, que evaluará si las condiciones del traslado solicitado son las idóneas para el debido funcionamiento de los equipos.

c) La reparación técnica de los equipos informáticos, que implique abrirlos o retirar las diferentes partes que lo componen, deberá ser realizada por la UTI. Cualquier cambio físico en los equipos debe ser evaluado y autorizado por la Jefatura de la UTI.

d) La conexión de dispositivos y partes (teclados, mouse, parlantes, impresoras, entre otros) diferentes a las entregadas en los equipos, es restringida, únicamente si se requiere para actividades laborales, deberá ser solicitada y supervisada por la UTI. Es competencia de la UTI, el retiro o cambio de partes.

e) Al momento de presentarse una falla de componentes físicos de un equipo informático, se verificará existencias en el mercado para realizar el reemplazo, en caso de estar desfasados y no existir para la reparación se procederá a dar de baja en el inventario; y se habilitará un equipo completo para uso del usuario o usuaria afectada.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

8.7 Política de uso de equipo informático

La adquisición de equipo informático será gestionada por la UTI en base a la naturaleza del cargo de la Unidad requirente, previa autorización de Gerencia. La UTI evaluará los requerimientos técnicos y consultará las alternativas por medio de un sondeo de mercado. La compra se realizará bajo la gestión y procesos establecidos por la Unidad de Adquisición y Contrataciones Institucionales. Como regla general, todo equipo que pertenece a la institución y/o utilice recursos informáticos dentro de la institución, podrán ser auditados por la UTI, ya sea con o sin previo aviso. Para el debido uso del equipo informático asignado, las y los usuarios se regirán por los siguientes lineamientos:

a) No se deberán utilizar disquetes, usb´s, cd´s, dvd´s, discos externos, tarjetas TFT o micro SD, entre otros, traídos de sitios externos a la institución, sin la previa revisión por parte del o la usuaria, por medio de la opción de exploración del antivirus instalado en la computadora asignada.
b) No se dará acceso total a dispositivos externos de almacenamiento masivo en las computadoras, esto para controlar la fuga de información, propiedad de la institución.
c) Evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo asignados.
d) La persona que tiene asignado equipos informáticos velará por el uso eficiente y eficaz de los mismos, así como de su protección, por lo que deberá apagarlos/desconectarlos en caso de no utilizarlos por periodos mayores a 4 horas, excluyendo de lunes a viernes el UPS, la UTI, supervisará y reportará a la Jefatura involucrada ante el incumplimiento.
e) En el caso de las Agencias Departamentales y Centros de Atención, las y los Encargados de Agencias deberán dejar apagado el equipo informático, excluyendo de lunes a viernes el UPS y los dispositivos de red conectados a este, los cuales deberán ser apagados únicamente para periodos de vacación largos o fines de semana, o según lo determine la UTI, que deberá proceder con las indicaciones del proveedor de los equipos, para evitar pérdidas de configuración o mal funcionamiento.
f) La Unidad de Logística y Activo Institucional, realizará revisiones periódicas que garanticen la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos

estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.

g) Informar oportunamente a la UTI, los eventos por mantenimientos eléctricos, daño en UPS, problemas al encender el equipo, que altere la continuidad de los procesos y actividades que requieren del uso del equipo informático. Deberá reportarse a la UTI, tan pronto se presente el problema, ya sea vía correo electrónico o ingreso de ticket o en caso que el equipo informático no se pueda encender realizarlo por medio de una llamada telefónica o en persona.

h) Los equipos informáticos deberán instalarse en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática, se deberán colocar en un espacio adecuado, cercanos a toma corriente y accesible para conexión de servicios de telecomunicaciones por parte de terceros. Se debe evitar el uso de regletas o extensiones que obstaculicen el libre tránsito en las oficinas de esta forma prevenir accidentes de trabajo.

i) Está prohibido colocar calcomanías en los equipos informáticos en general, papelería, artículos de oficina u objetos en el espacio de trabajo o mobiliario asignado para el equipo informático.

j) Queda prohibido ingerir alimentos en los puestos de trabajo donde se encuentra instalado el equipo informático.

k) La o el usuario deberá asegurar la limpieza superficial del área de trabajo o mobiliario donde se encuentra instalado el equipo informático, para evitar acumulación de polvo, de esta forma resguardar el equipo y colaborar con la actividad de mantenimiento informático que realiza el personal de la UTI asignado.

l) Los equipos informáticos, periféricos o accesorios asignados por la UTI, que sufran algún desperfecto, daño por mal uso, descuido o negligencia por parte del o la usuaria responsable, se le levantará un reporte por incumplimiento de las presentes políticas, el cual se hará llegar a la Jefatura inmediata.

m) Los equipos portátiles o laptop, que requieran ser utilizados fuera de las instalaciones de Oficina Central o movilizarse internamente, son de responsabilidad directa de la persona usuaria al que han sido asignados, la UTI no es responsable de mover los equipos portátiles o laptop, únicamente proporcionará asistencia de conexión de red, acceso a impresora o verificación del funcionamiento del equipo, en caso sea requerido por la o el usuario. A excepción de los equipos proyectores y laptop que administra directamente la UTI.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

n) Los equipos portátiles o dispositivos informáticos personales en general, que las y los usuarios tengan en uso dentro de las instalaciones de la institución no se les brindará soporte de ninguna índole, esto incluye: acceso a la red interna, ya sea uso de impresoras o internet, reparaciones, ayuda con funcionamiento o revisiones generales de hardware, ni de software, ya que no corresponde a la UTI adquirir responsabilidad por equipos o dispositivos informáticos que no son propiedad de la institución. Son de responsabilidad directa del adquiriente.

o) No se deberá realizar traslado de información oficial de trabajo almacenada en los equipos informáticos propiedad de la Institución, hacia equipos portátiles personales.

p) Las y los usuarios no están autorizados para realizar formateos de disco duro o extracción completa de información en medios de almacenamiento externo (USB, discos duros externos, etc.) de las computadoras asignadas, es la UTI la que realizará esta actividad, haciendo previamente un respaldo de una información.

q) Está prohibido para los usuarios hacer uso irracional y desconsiderado del espacio disponible en disco duro de los equipos, acumulando material que no está relacionado con el aspecto laboral, sean estos: vídeos, películas, música, fotos, etc. provenientes de Internet o de otros medios que no estén relacionados con sus funciones laborales.

r) La Unidad de Desarrollo Humano debe reportar a la UTI, el personal que cesa sus actividades, la UTI al ser informado, realizará una copia de respaldo integral del equipo asignado en un mínimo de 2 días antes a la fecha del cese de las actividades, este proceso será auditado por la Jefatura de Auditoría Interna.

s) La UTI recibirá el equipo por parte de la persona que cesa sus actividades, realizará el inventario tomando de base la última hoja de inventario de hardware y software firmada por ella, elaborando un acta con el detalle de lo recibido, la cual deberá ser firmada por esta.

t) Los traslados o cambios de ubicación por nuevas asignaciones para los equipos informáticos, se realizarán únicamente si se encuentran en buenas condiciones y cumplen con las características técnicas según se requiera para que puedan cumplir sus tareas en forma eficiente y a la vez optimizando los recursos. Este proceso se realizará con autorización de Gerencia y la Jefatura de UTI; respaldado por el respectivo "Formato de Traslado", se entregará copia a la o el usuario y a la Unidad de Logística y Activos.

u) El equipo y dispositivos informáticos será asignado en uso a una persona en particular, quien firmará acta de recibido post-entrega. En el caso que los equipos o dispositivos informáticos sean utilizados por más de una persona, la responsabilidad recaerá sobre quien firmó el acta.

v) La Unidad de Participación Ciudadana, Publicidad y Comunicaciones, será la encargada de diseñar y enviar vía correo, en formato .jpg, los fondos de pantalla, conmemorativos al mes correspondiente o a festividades, a la UTI para que sea aplicado al servidor de dominio y este refleje a todas las computadoras por medio de la "Política de Fondo de Pantalla" y que sean homogéneos para todos los usuarios de la institución.

w) Cualquier persona que tenga acceso a las instalaciones de La Caja, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual tendrá que retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente, con el visto bueno de la Jefatura de la UTI y autorización de Gerencia.

8.8 Política de gestión de copias de seguridad o respaldo de información

La UTI es responsable de realizar respaldos de la información contenida en los equipos de trabajo y de las bases de datos de sistemas contenidas en servidores, ya que representan un activo valioso para la institución, en la ejecución de los procesos de atención a la población usuaria y en la toma de decisiones. La UTI mantendrá registros de información relaciona a las actividades laborales del personal que posea un alcance de tipo institucional, identificando el grado de relevancia de los datos en la continuidad de los procesos operativos, definiéndose en alta, media o baja, para establecer el medio de resguardo, la periodicidad y el tiempo requerido de almacenamiento.

Respaldo de información de computadoras:

a) Los respaldos en Oficina Central, se realizarán de forma automática por medio de software, que permita crear tareas periódicas de copias de seguridad de las carpetas seleccionadas en los equipos y transferirlas a un servidor dedicado para el almacenamiento de respaldos, instalado en la red, considerando las características de la información a respaldar. Estableciéndose respaldos parciales o completos.

- Importancia Alta: Se planificará el respaldo diario en horario de baja demanda de la red de datos.
- Importancia Media: Se planificará la tarea de respaldo de 2 a 3 días a la semana en horario de baja demanda de la red de datos.
- Importancia Baja: La tarea de respaldo se definirá 1 vez cada semana, cada 15 días o una vez al mes.
- Se realizará copia de respaldo de documentos automáticamente según planificación de tarea a la carpeta de perfil del usuario ubicada en la unidad D: de cada equipo, por lo que será responsabilidad de cada usuario que almacene toda la información en dicha carpeta.

La UTI, no se hará responsable por perdidas de datos que no estén almacenados en la ubicación establecida.

b) La UTI deberá contar con los mecanismos y herramientas necesarias para poder implementar de manera automática los respaldos de información, así como con los dispositivos de almacenamiento en caso de ejecutar dicho proceso de forma manual.

c) La UTI realizar el proceso de configuración de tareas programadas de copias de seguridad, deberá documentar por cada equipo informático, una bitácora del estado de los respaldos, realizando revisiones trimestrales para verificar el funcionamiento de la herramienta de software, las incidencias presentadas, para establecer controles y auditorías.

d) El personal de la UTI que realice la tarea de respaldo, deberá enviar por correo electrónico, copia de las bitácoras de ejecución a la Jefatura de la UTI, con un informe resumen por equipo de las incidencias e indicando el estado de los respaldos por cada computadora.

e) Los respaldos de información de las computadoras de Agencias Departamentales y Centros de Atención, se realizarán en la visita de Soporte Técnico Informático según programación establecida. Los medios de almacenamiento externos en los que se respalde la información serán administrados y resguardados por la UTI, que los trasladará manualmente al servidor dedicado.

f) Se excluirá de los respaldos la información que se catalogue como no relevante, que no formen parte de las actividades laborales asignadas por la institución, incluyendo: videos, música, fotografías, documentos personales. La o el usuario de la computadora deberá eliminar o trasladar a un medio de almacenamiento propio la información personal, ya que no deben ocupar espacio en el disco duro de la computadora asignada por la institución.

g) Se realizarán respaldos de información por medio de copias de seguridad en formato de imagen de disco o particiones en caso de mantenimiento correctivo, resguardando la información en los medios de almacenamiento externos administrados por la UTI.

h) En caso de colocar claves a archivos institucionales, la persona usuaria deberá entregar en un sobre sellado la respectiva clave, el nombre del archivo y la ruta de almacenamiento del mismo así como la fecha de entrega del sobre, para que sea resguardada en La Caja fuerte de la UTI, y deberá entregar un sobre tantas veces como haga una modificación en la clave del archivo.

i) Las y los usuarios que requieran realizar respaldos de información de manera descentralizada de la UTI, lo realizará en un dispositivo de almacenamiento propio y deberán solicitar autorización a la o el Jefe de la Unidad, por escrito, justificando el motivo del requerimiento. El proceso deberá ser auditado por la UTI.

j) Los respaldos de los datos de usuario no podrán ser eliminado o destruidos, sin autorización de la Jefatura de la UTI.

Copias de seguridad de base de datos:

k) Los respaldos de base de datos se programarán automáticamente de forma incremental todos los días de la semana, a las 11:30 pm, por medio de la herramienta de software centralizado, compatible con el gestor de base de datos, que permita la administración de recursos de almacenamiento para la generación de copias de seguridad.

l) Se realizarán de lunes a viernes, a las 6:00 am, traslados automáticos a cintas magnéticas de almacenamiento para ser resguardadas por el tiempo que se estime conveniente.

m) Se realizarán cada 3 meses pruebas de restauración de datos desde respaldos, para validar la integridad de los datos, evitando inconsistencias o que no sea utilizable en caso de requerirse procesos de recuperación por contingencia o por desastres.

n) La UTI administrará y monitoreará la herramienta de software de respaldos de bases de datos, realizará revisiones diarias del estado de los respaldos de las bases de datos. Deberá enviar vía correo electrónico un informe mensual del estado de los respaldos a la Jefatura de la UTI.

o) Las copias de seguridad de las bases de datos no podrán ser eliminado o destruidos, sin autorización de la Jefatura de la UTI.

CAJA DE EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

8.9 Política de uso de impresores y periféricos

La UTI en coordinación con las Jefaturas de Unidades, es la responsable de analizar y evaluar la factibilidad de habilitar equipos de impresión y escaneo en puntos o unidades estratégicas de la institución, de acuerdo a las necesidades específicas de cada usuario o usuaria y la disponibilidad de los mismos, en base a los siguientes puntos:

a) Las y los usuarios deberán hacer buen uso de los impresores, no imprimiendo documentos personales que no tengan ninguna relación con las actividades labores. Asimismo, deberá revisar el documento antes de imprimirlo para hacer las correcciones necesarias, evitando así generar desperdicios de recursos. La UTI llevará un control de las impresiones por cada persona usuaria y entregará un reporte mensual de las impresiones a Gerencia o cuando ésta lo solicite.
b) Las impresoras en red están configuradas como compartidas, pueden ser utilizadas por todo el personal de la institución, según la asignación que se realice respetando el área o grupo de trabajo donde se encuentren instaladas, esto con el fin de tener un control y uso eficiente de los suministros de impresión.
c) Cuando la impresora y/o escáner presente problemas, se deberá dar aviso a la UTI para que el personal técnico pueda solucionar el problema inmediatamente o en caso de ser un equipo gestionado por arrendamiento solicitar la asistencia de la parte técnica asignada por el proveedor, por medio del administrador de contrato.
d) La reparación y los tiempos de respuesta de las impresoras de inyección, láser y matriciales de las Agencias Departamentales y Centros de Atención, que no posean contrato de mantenimiento, dependerán del proceso interno de gestión de compra de las partes a reemplazar para restablecer el equipo, por parte del personal de la UTI. La o el Encargado de Agencia o Centro de Atención, deberá informar la problemática por medio de correo electrónico a la Jefatura inmediata, quien dará parte a la Jefatura de la UTI.

8.10 Política de ingreso al área de servidores

La UTI es la responsable de coordinar y autorizar los accesos al área de servidores y equipo de telecomunicaciones, para lo cual se tendrán las siguientes consideraciones:

a) El acceso al área de servidores es exclusivo para personas autorizadas por la Jefatura de la UTI, previo aviso por medio correo electrónico informando el motivo del ingreso.
b) Se llevará una hoja de control de acceso de las personas externas que ingresen al cuarto de servidores, agregándolas los siguientes datos: fecha de ingreso, hora de entrada y salida, nombre completo, número de documento de identificación, motivo del ingreso y firma.
c) Las personas externas o personal interno que solicite ingresar al área de servidores deberán ser supervisado, en todo momento, por personal de la UTI hasta finalizar las actividades requeridas e informadas a la Jefatura de la UTI.
d) Las llaves de ingresos serán resguardadas por la Jefatura de la UTI, entregándoselas al personal de la UTI cuando se requieran, que deberá informar la actividad a realizar en el lugar. Queda a consideración de la Jefatura de la UTI, llevar el control de las personas a las que proporciona las llaves.
e) Las personas externas que requieran acceso al área de servidores deberán registrar el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento o herramientas que requieran para realizar las actividades de trabajo en dicha área.

8.11 Política de mantenimiento preventivo y correctivo de equipos informáticos

La UTI es la única autorizada a realizar las actividades de soporte técnico y cambios de configuración en los equipos informáticos. En el caso que se requieran labores de mantenimiento efectuadas por terceras personas estas deben ser previamente aprobadas por la Jefatura de la UTI. Para los equipos informáticos en general con esquema de arrendamiento, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware/software, con la supervisión de la UTI, o según indicaciones de la Jefatura de la UTI. Por tanto, el mantenimiento preventivo y correctivo de los equipos informáticos institucionales, se realizará bajo los siguientes lineamientos:

a) El personal de la UTI designado para realizar las actividades de mantenimiento preventivo, deberá presentar a la Jefatura de la UTI, el "Programa Anual de Mantenimiento de Equipos Informáticos" al inicio del año en curso, los cuales se realizarán 4 veces al año.

b) La o el usuario del equipo informático es responsable de otorgar las facilidades, así como el tiempo requerido para poder dar el servicio preventivo o correctivo, por parte del personal de la UTI designado.

c) En caso de que no se facilite el equipo informático en la fecha definida para realizar el servicio preventivo o correctivo, deberá escribir el motivo y firma en la hoja de "Rutinas de Mantenimiento de Equipo Informático", solicitando la reprogramación y definiendo la fecha a realizarse, que no deberá de pasar de 3 días posteriores.

d) El mantenimiento preventivo en Agencias Departamentales y Centros de Atención, se coordinará con las y los Responsables, la fecha de visita y se informara a la Jefatura de Comercialización.

e) De necesitar mantenimiento correctivo por falla en el equipo de informático, el usuario deberá informar la problemática presentada, vía teléfono o verbal a la UTI, para que a la brevedad posible se realice la revisión y se proporciona solución, según corresponda.

f) En caso de presentarse la necesidad de reemplazar alguna pieza, que se ha detectado dañada del equipo de informático al momento de realizar el mantenimiento preventivo, el personal de la UTI, elaborará un informe con la problemática detectada, para solicitar la compra de la(s) pieza(s) a reemplazar para reparar el equipo y dejarlo funcionando de manera óptima. El informe será revisado por la Jefatura de la UTI y la compra autorizada por Gerencia. Si el monto de la pieza a adquirir no sobrepasa el monto máximo Chica, se solicitará por esta, en caso contrario se realizará la gestión de compra sujetos al proceso de la Unidad de Adquisiciones y Compras Institucionales.

g) La UTI deberá tener los suministros e implementos necesarios para realizar la actividad de mantenimiento preventivo y correctivo de equipos informáticos.

8.12 Política de desarrollo y actualizaciones de sistemas informáticos

Esta política tiene como objetivo establecer los lineamientos que se aplicarán durante el proceso de desarrollo y actualización (local y externo) de los sistemas informáticos, así como los mecanismos que permitan establecer controles de seguridad y validación de datos en el desarrollo de los mismos.
Para su asignación y uso se deberán cumplir los siguientes lineamientos:

a) La UTI es la encargada de la metodología para la implementación del ciclo de vida del desarrollo de los sistemas informáticos (desarrollo local y externo), asegurando que los sistemas sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajusten al cumplimiento de leyes, reglamentos y normativas vigentes que sean aplicables a la institución.
b) Al contratar servicios tecnológicos con terceros, la UTI, deberá justificar la tercerización del servicio de software, siendo responsable de administrar los aspectos técnicos en la adquisición de los bienes y/o servicios de tecnología de información y comunicaciones. La UTI deberá realizar una efectiva administración del riesgo, considerando acuerdos de confidencialidad, contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, entre otros; además, mantener una metodología estándar de desarrollo y adquisición de software, realizado por terceros.
c) La UTI deberá definir una adecuada separación de los ambientes de desarrollo y de producción. El personal encargado del desarrollo de software, deberá trabajar en un ambiente de desarrollo, que permita la validación de datos de entrada, procesamiento interno y salida de datos.
d) El acceso a las bases de datos en etapa de diseño, de prueba y en producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). En la etapa de construcción y/o prueba no se debe dar acceso a los datos de producción.
e) La UTI, debe asegurar y realizar, el análisis e implementación de los requerimientos de seguridad de software y/o sistemas de información que se desarrollen o se adquieran, debe incluir controles

de autenticación y auditoría de usuarios, verificación de los datos de entrada y salida, y que se implementen buenas prácticas para un desarrollo seguro.

f) La UTI, deberá contar con políticas y procedimientos para el procesamiento de la información, desde su origen, relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que la información sea completa, precisa, confiable y válida para la toma de decisiones.

g) La UTI, deberá crear y actualizar, manuales de usuario y técnico, para el uso de los sistemas en producción; documentar el control de cambios (versiones de Sistemas).

h) El acceso a la documentación de los sistemas informáticos, bibliotecas de códigos fuentes y programas ejecutables, debe estar restringida sólo a personas autorizadas. La excepción a esta política, son los manuales de usuario, u otros documentos destinados a las personas usuarias de los sistemas informáticos.

i) El código fuente de los sistemas informáticos desarrollados internamente son propiedad de La Caja, el personal de la UTI deberá resguardarlo y abstenerse a hacer uso o comercializarlo fuera de la institución.

8.13 Política de asignación, uso y control de teléfono móvil institucional

Esta política tiene como objetivo establecer los lineamientos para regular la asignación y uso de teléfonos celulares, cuya adquisición y utilización es financiada con recursos de La Caja, por tanto son propiedad de la institución, los cuales servirán al personal como herramienta de comunicación para brindar un mejor servicio a los afiliados, optimizar los tiempos de respuestas en la comunicación interna, así como de apoyo oportuno para las operaciones administrativas de La Caja. Para su asignación y uso se deberán cumplir los siguientes lineamientos:

a) La UTI realizará la gestión para el contrato anual de "Servicios de Telefonía Móvil".

b) La UTI deberá contar con las herramientas de seguridad y mecanismos de prevención necesarios para el control y supervisión de los dispositivos móviles, para verificar el uso óptimo de los servicios proporcionados.

c) Las Jefaturas de las diferentes unidades realizarán la solicitud de asignación de líneas telefónicas móviles para el personal a cargo, según las necesidades operativas. Presentarán por escrito o vía

correo, a la Jefatura de la UTI el requerimiento de líneas telefónicas por usuario, justificando su uso en el formato de "Solicitud de asignación o renovación de equipo celular".

d) Las y los usuarios sólo utilizarán el teléfono celular para fines oficiales, como herramienta de trabajo, observando un uso adecuado y responsable del mismo. Deberán portarlo consigo durante la jornada laboral y fuera de esta en territorio nacional, debiendo mantenerlo encendido las 24 horas del día por cualquier emergencia, con la discreción inmediata para contestarlo.

e) Las características de los teléfonos móviles asignados al personal, deberán ser acorde a las funciones y tareas laborales a desempeñar.

f) Cada línea telefónica asignada deberá contar con un plan de minutos al mes, de acuerdo al plan que se contrate con la empresa de servicios telefónicos, con un monto de consumo máximo autorizado por el Consejo Directivo de La Caja. El monto podrá ser distribuido en diferentes servicios: telefonía móvil, internet o mensajería instantánea. En caso de exceder el monto establecido, es responsabilidad del Empleado cancelarlo, por medio de descuento en la planilla de sueldos correspondiente al siguiente mes de haberse recibido la factura de consumo.

g) En caso de mal funcionamiento del teléfono móvil, este deberá reportarse de inmediato al Administrador de Contrato designado, que realizará el trámite con la Empresa suministrante, para su revisión y reparación. En caso de extravío, deterioro por mal uso o robo; la o el usuario deberá reportarlo inmediatamente, directamente a la empresa suministrante y al Administrador de Contrato designado, además presentará la denuncia a la Policía Nacional Civil, entregándole al Administrador de Contrato una copia de la denuncia correspondiente, a más tardar 24 horas después de interpuesta, para que gestione el respectivo seguro.

h) La o el usuario es responsable de realizar los trámites requeridos y realizar la cancelación por el deducible del dispositivo móvil a la empresa suministrante; en caso de no contar con seguro que cubra el riesgo de extravío, deterioro por mal uso, el responsable del teléfono móvil, pagará el total del costo del teléfono móvil, en un período no mayor de ocho días calendario. Esto con el objetivo de garantizar la comunicación institucional. En caso, que el Empleado no cancele el deducible del seguro o el costo total del teléfono móvil, será cancelado por La Caja y se le descontará en el salario próximo a la fecha de finalización de los ocho días.

i) La UTI es la responsable de realizar la entrega del teléfono móvil al personal, que deberán verificar los accesorios recibidos.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.

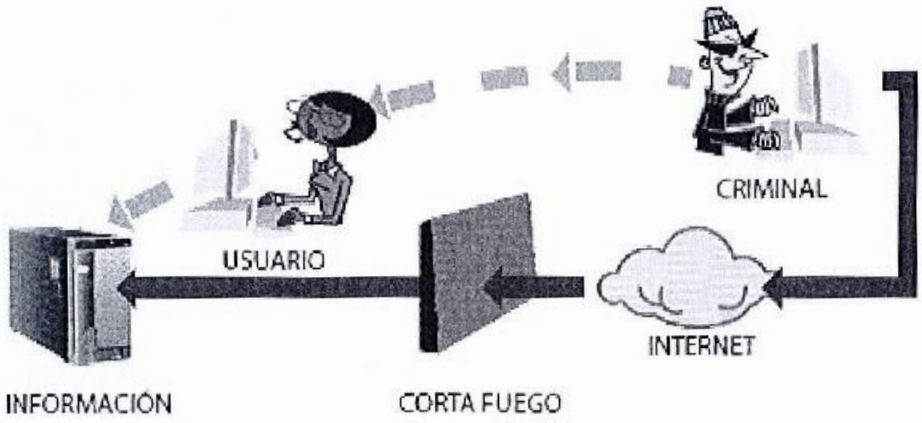
j) A cada teléfono móvil nuevo, la UTI, le realiza las siguientes configuraciones:

- Habilitar el SIM con el número de teléfono asignado.
- Asignar un pin o patrón de seguridad.
- Contactos del personal de la Caja Mutual.
- Configuración de la cuenta de correo institucional.
- Instalación de la aplicación para móvil de Seguros, para uso del personal de las Agencias Departamentales y Centros de Atención.
- Instalación de antivirus y aplicaciones requeridas para el uso óptimo y seguro de la información que se transfiere por medio de los dispositivos móviles.

k) Cada usuario o usuaria es responsable de asignar un PIN de bloqueo del dispositivo móvil, que permita resguardar los datos e información de La Caja que portan en el teléfono móvil.

El adecuado uso de los servicios y recursos de las tecnologías de información y comunicaciones de La Caja, son de responsabilidad directa de sus usuarios, ya que representan el eslabón más débil en la cadena de seguridad. El factor determinante de la seguridad informática de las instituciones, es la capacidad de los usuarios de interpretar correctamente las políticas de seguridad y hacerlas cumplir.

UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN DE LA CAJA.



CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
JEFE DE TECNOLOGÍAS DE INFORMACIÓN
EL SALVADOR, C.A.