CAJA MUTUAL DEL ABOGADO DE EL SALVADOR – CAMUDASAL San Salvador

MANUAL DE POLITICAS Y PROCEDIMIENTOS SOBRE LOS CONTROLES GENERALES DE LOS SISTEMAS DE INFORMACION DE CAMUDASAL.

APROBADO EN ACTA CD 36/2013.

2018

CAMUDASAL
TÉCNICO INFORMÁTICO
Francisco Yohalmo Valdéz

Title

Subtitle

Author

Date

APROBADO EN ACTA CD 36/2013

EL CONSEJO DIRECTIVO DE LA CAJA MUTUAL DEL ABOGADO DE EL SALVADOR.

CONSIDERANDO:

I) Que para cumplir con los fines, atribuciones y objetivos de la mencionada Ley, es necesario dictar las normas que regulen las funciones de la Caja y las diversas materias que la integran.
II) Con el objetivo de regular las operaciones de crédito entre la Caja Mutual del Abogado de El Salvador y el afiliado y en uso de las facultades establecidas en el articulo 16 literal c), de la Ley del Régimen de Previsión y Seguridad Social del Abogado de El Salvador, ACUERDA:

APRUEBASE, el siguiente:

MANUAL DE POLITICAS Y PROCEDIMIENTOS SOBRE LOS CONTROLES GENERALES DE LOS SISTEMAS DE INFORMACION DE CAMUDASAL

GENERALIDADES

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades Institucionales en materia de seguridad, que garanticen la continuidad en la prestación eficiente de los servicios que se ofrecen.

Este documento se encuentra estructurado en siete políticas generales de seguridad para usuarios de informática, que consideran los siguiente puntos:

- Seguridad de Personal
- Seguridad Física
- Seguridad Lógica de la RED

- Seguridad de Controles de Acceso Lógico
- Seguridad para la Administración de los Recursos de Computo
- Seguridad para el Usos de Servicios de RED
- Seguridad para el Uso de Antivirus de RED

Objetivo
Establecer y difundir las Políticas y las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, Bases de Datos, Redes) y se aplican a todos los usuarios de cómputo de la Caja Mutual del Abogado de El Salvador (Camudasal) para que sea de su conocimiento y cumplimiento para proteger adecuadamente los activos tecnológicos asignados y la información de la Empresa para el eficiente desempeño de sus funciones en PRO de los fines Institucionales.

Alcance
El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios (Funcionarios y Empleados) para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del la Caja Mutual del Abogado de El Salvador (Camudasal).

Base Legal
Las Normas Técnicas de Control Interno Específicas de Camudasal en el Art. 27.- demandan implementa un Manual sobre Políticas y Procedimientos de Controles Generales de los Sistemas de Información.
La Ley del Régimen de Previsión y Seguridad Social del Abogado establece como atribuciones del Consejo Directivo: Emitir los manuales, circulares y demás disposiciones que fueren necesarias para el mejor funcionamiento de La Caja

Beneficios
Las Políticas y Estándares de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos y sistema de información de Camudasal.

Incumplimientos
Cualquier acción que vaya en contra de las políticas de seguridad Informática de la Caja Mutual del Abogado de El Salvador deberá ser sancionada por la Gerencia correspondiente y con conocimiento del Consejo Directivo en una primera ocasión y de manera indefinitiva con terminación de contrato del usuario responsable en caso de reincidencia y daño grave a los sistemas y equipos.

CAJA MUTUAL DEL ABOGADO DE EL SALVADOR – CAMUDASAL – San Salvador

CAPÍTULO 1
POLÍTICAS DE SEGURIDAD DEL PERSONAL

1.1 Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y normas establecidas en el presente Manual de Políticas y Procedimientos sobre Sistemas Generales de Información.

1. 2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos de Camudasal deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información Institucional, así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Procedimientos sobre Sistemas Generales de Información.

1.3 Entrenamiento en Seguridad Informática

Todo empleado o funcionario de Camudasal de nuevo ingreso deberá:
Leer el Manual de Políticas y Procedimientos sobre Sistemas Generales de Información, donde se dan a conocer las obligaciones para los usuarios. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

CAPÍTULO 2
POLÍTICAS SEGURIDAD FÍSICA

2.1 Acceso Físico

Todo el equipo de cómputo y medios de comunicación estarán debidamente protegidos con la infraestructura apropiada.

El acceso a la sala donde se ubican los servidores debe ser restringido y solo podrán acceder el personal de informática y personas autorizadas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el Encargado de Informática con el consentimiento del usuario; para lo cual puede implementarse formatos de Entrada/Salida, notificando al Encargado de Bienes de Activo Fijo y al personal de seguridad.

2.2 Robo, pérdida o transferencia de equipo

El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo; a excepción del equipo destinado para eventos, seminarios, presentaciones, promoción de servicios y otros, para lo cual el responsable del equipo autorizará formalmente su uso al personal que participe en dichos eventos haciendo uso de los formatos de Entrada/Salida

El usuario deberá dar aviso de inmediato a la Gerencia de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.3 Protección Física

2.3.1 La sala de servidores debe:

- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Ser un área restringida.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Contar por lo menos con un extintor de incendio adecuado y cercano
- Se deberá tener fácil acceso a los procedimientos de contingencias.

2.3.2 Los usuarios no deben mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la gerencia o a quien esta designe, debiéndose solicitar a la misma en caso de requerir este servicio.

2.3.3 El Encargado de Bienes de Activo Fijo entregara formalmente los equipos a los usuarios mediante el formulario de asignación de bienes; dejando bajo su responsabilidad los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Gerencia.

2.3.4 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas a los empleados o funcionarios de La Caja

2.3.5 Es responsabilidad de los usuarios almacenar su información únicamente en el servidor que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo, red, correos, servicio Web.

2.3.6 Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico o recipientes con tapa.
2.3.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.
2.3.8 Se debe mantener el equipo informático en un entorno limpio y sin humedad.
2.3.9. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.
2.3.10 Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados a la Gerencia con una semana de anticipación a través de un plan detallado de movimientos debidamente autorizados.
2.3.11 Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo o corre el riesgo de dañarlos; esto es exclusivo del Encargada de Informática o personal de mantenimiento.

2.4 Respaldos

Las Bases de Datos de Camudasal serán respaldadas semanalmente en forma automática y manual, según los procedimientos generados para tal efecto.
Las copias de respaldos deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

2.5. Mantenimiento de equipo

2.5.1. Únicamente el personal autorizado por la Dirección o Gerencia podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.
2.5.2. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación.
2.5.3 El encargado Informática será responsable de calendarizar y organizar el mantenimiento preventivo y correctivo de los equipos de cómputo

CAPÍTULO 3
POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED DE CAMUDASAL

3.1 De la Red

La Red de la Camudasal tiene como propósito principal servir en la transformación e intercambio de información dentro de la entidad entre usuarios, técnicos y unidades.

3.1.1 Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

3.1.2 No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus superiores correspondientes.

3.1.3 No se permite el uso de los servicios de la red cuando no cumplan con los quehaceres propios de la empresa.

3.1.4 Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de Camudasal y se usarán exclusivamente para actividades relacionadas con la Institución.

3.1.5 Todas las cuentas de acceso a los sistemas y recursos de Informática son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos de usuario.

3.1.6 El uso de analizadores de red es permitido única y exclusivamente por el personal de Informática, para monitorear la funcionalidad de la Red, contribuyendo a la consolidación del sistema de seguridad.

3.2 Del área de Informática

3.2.1 El Encargado de Activo Fijo debe llevar un control total y sistematizado de los recursos de cómputo

3.2.2 El encargado de personal informará el Encargado de Informática cuando un usuario deje de laborar o de tener una relación con la empresa a efectos que se desactiven su usuario y passwords de acceso a redes o sistemas.

3.2.3 Si un usuario o departamento viola las políticas vigentes de uso aceptable de la Red de Camudasal, el administrador de la Red lo notificara a la Gerencia para la imposición de las sanciones correspondientes.

3.2.4 Para reforzar la seguridad de la información de los usuarios, bajo su criterio, deberá hacer respaldos de la información en sus discos duros dependiendo de la importancia y frecuencia del cambio de la misma.

3.2.5 Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

3.2.6 El Encargado de Soporte Técnico es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, Los empleados que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir al Encargado de Informática, para solicitar asesoría al respecto.

3.3 Políticas de uso aceptable de los usuarios

3.3.1 Los recursos de cómputo empleados por el usuario:

Deberán ser afines al trabajo desarrollado
No deberán ser proporcionados a personas ajenas
No deberán ser utilizados para fines personales

3.3.2 Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.
3.3.3 Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.
3.3.4 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red, de acuerdo con las políticas que en este documento se mencionan.
3.3.5 Los usuarios deberán solicitar apoyo al encargado de Informática ante cualquier duda en el manejo de los recursos de cómputo de la institución.

3.4 Uso del correo electrónico

3.4.1 Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si un usuario recibe mediante correo información importante de índole institucional, se autoriza recepción de copia a otro usuario debidamente identificado.
3.4.2 Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de Camudasal. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
3.4.3 La Empresa, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal a efectos de verificar el buen uso del correo institucional asignado.
3.4.5 El usuario debe de utilizar el correo electrónico de Camudasal, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.
3.4.6 La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la Gerencia , señalando los motivos por los que se desea el servicio. Esta solicitud deberá darse a conocer al Encargado de Informática.
3.4.7 Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
3.4.8 El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).
3.4.9 Para reforzar la seguridad de la información de su cuenta, el usuario –conforme su criterio- deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos de la información de la cuenta serán responsabilidad absoluta de los usuarios.
3.4.10 El Encargado de Informática se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
3.4.11 Una cuenta de correo electrónico institucional deberá estar conformada por nombre del puesto de trabajo y solo podrá acceder desde su equipo de trabajo, por lo cual la contraseña estará asignada en el equipo por el Encargado del Sistema.
La sintaxis de la cuenta de correo será: nombre del puesto @camudasal.gob.sv. (1)

3.4.12 La cuenta será creada y activada por el Encargado de Informática, una vez reciba autorización de asignación de cuenta de correo al usuario.

3.5 De los servidores de la Red de Camudasal.

3.5.1 El Encargado de Informática tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

3.5.2 Durante la configuración del servidor el Encargado de Informática debe normar o al menos comunicar mediante correo electrónico o memorando el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios

3.5.3 Los servidores que proporcionen servicios a través de la RED e Internet deberán:

Funcionar 24 horas del día los 365 días del año.
Recibir mantenimiento preventivo máximo cuatro veces al año.
Recibir mantenimiento semestral que incluya depuración de bitácoras.
Recibir mantenimiento anual que incluya la revisión de su configuración.

3.5.4 La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

Semanalmente, información crítica como la base de datos.
Semanalmente documentos alojados por los usuarios en los servidores correspondientes.
Semanalmente, los correos y los documentos Web.
Mensualmente, configuración del servidor y bitácoras.

3.5.5 Los servicios institucionales hacia Internet sólo podrán proveerse a través de los servidores autorizados por el Encargado de Informática.

3.5.6 Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones:

Acceso restringido.
Temperatura adecuada al equipo.
Libre de polvo
Protección contra descargas eléctricas.
Mobiliario adecuado que garantice la seguridad de los equipos.

CAPITULO 4
POLÍTICAS DE CONTROLES DE ACCESO LÓGICO

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información de la RED de Camudasal, por lo cual deberá mantenerlo de forma confidencial.

La Gerencia por medio del Encargado de Informática, es el único que puede determinar y autorizar el tipo de información al que pueden tener acceso los usuarios, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

4.1. Controles de acceso lógico

4.1.1 Solo los empleados, funcionarios y equipo técnico de Informática tendrá el acceso a la información de la RED Institucional; para personal externo debe ser autorizado al menos por la Gerencia con la aprobación del Encargado de Informática, quien lo habilitará.

4.1.2 Cada usuario únicamente tendrá acceso a los recursos de la Base de Datos de conformidad a los niveles de información según su perfil de usuario respondiendo a su puesto de trabajo; esto es a nivel de administrador, consulta y alimentación o modificación del ambiente de trabajo.

4.1.3 Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a los sistemas y la RED de Camudasal, a menos que se tenga autorización de la Dirección.

4.1.5 Cada usuario que accede a la infraestructura de sistemas y la RED de Camudasal debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.6 Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.7 Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de privilegios

4.2.1. Cualquier cambio en los perfiles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura de información de la Empresa, deberán ser notificados por escrito o vía correo electrónico a la Gerencia con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.2.2 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados por el personal responsable, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.3 Administración y uso de contraseñas

4.3.1 La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

4.3.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo al Encargado de Informática, indicando si es de acceso al equipo o a módulos de sistemas de la RED, para que se le proporcione una nueva contraseña.

4.3.3 La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Dirección como empleado de Camudasal.

4.3.4 Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que no se permita a personas no autorizadas su conocimiento.
4.3.5 Las contraseñas de acceso a los sistemas y la RED para los usuarios deberán observar los siguientes lineamientos:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10).Estos caracteres deben ser alfanuméricos, o sea, números y letras;
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.3.6 Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.
4.3.7 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.
4.3.8 En caso de olvido de contraseña de un usuario, será necesario que se presente con el Encargado de Informática para reasignarle su contraseña. Los cambios o desbloqueo de contraseñas se harán ante el mismo de ser posible por escrito.

4.4 Permisos de uso de Internet

4.4.1 El acceso a Internet provisto será a nivel de jefaturas y será exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
4.4.2 La asignación del servicio de Internet, deberá solicitarse por escrito a la Dirección, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente. Si un empleado que no tenga calidad de jefe considera necesario el uso de Internet deberá solicitarlo en la misma forma y será el jefe inmediato junto a la Gerencia quines analizaran y autorizan dicho servicio.
4.4.3 Los usuarios con acceso a Internet tienen que reportar todos los incidentes de seguridad informática al Encargado del área, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
4.4.4 El acceso y uso de módem tiene que ser previamente autorizado por la Dirección.
4.4.5 Los usuarios con servicio de navegación en Internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Dirección.
- La utilización de Internet es para el desempeño de su función y puesto de trabajo y no para propósitos personales.

4.4.6 Los esquemas de permisos de acceso a Internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de Internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.

NIVEL 3: Internet restringido y sin mensajería instantánea: Los usuarios sólo podrán hacer uso de Internet aplicándose las políticas de seguridad y navegación

NIVEL 4: El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

4.5. Control de accesos remotos

4.5.1 Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Administración.

4.5.2 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Administración.

4.6 De los Sistemas Institucionales de Información

4.6.1 El Administrador de la Base de Datos (ABD) tendrá acceso a la información de la Base de Datos únicamente para:

La realización de los respaldos de la BD.

Solucionar problemas que el usuario no pueda resolver.

Diagnóstico o monitoreo.

4.6.2 El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

4.6.3 El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso. Para tal efecto será necesario seguir el procedimiento determinado para tal efecto.

4.6.4 Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable.

4.6.5 En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

CAPÍTULO 5
POLÍTICAS DE SEGURIDAD LÓGICA PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO

5.1 Área de Seguridad en Cómputo

5.1.1 El Encargado de Informática es la encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.

5.5.2 El Encargado de Informática debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

5.1.3 El Encargado de Informática es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

5.1.4 El personal de informática dará soporte técnico únicamente al equipo de cómputo de la entidad

5.2 Administradores de Equipos y RED

5.2.1 El Encargado de Informática deberá notificar a la Gerencia y este imponer medidas disciplinarias a los usuarios en los siguientes casos:

- Si la cuenta no se está utilizando con fines institucionales.
- Si pone en peligro el buen funcionamiento de los sistemas.
- Si se sospecha de algún intruso utilizando una cuenta ajena.
- Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
- Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
- Si se detectan accesos no autorizados que comprometan la integridad de la información.
- Si se viola las políticas de uso de los servidores.
- Si se reporta un tráfico adicional que comprometa a la red de la Entidad.

5.2.2 El Encargado de Informática deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

5.2.3 El Encargado de Informática deberá realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

5.2.4 El Encargado de Informática debe actualizar la información de los recursos de cómputo de la entidad, cada vez que adquiera e instale equipo o software.

5.2.5 El Encargado de Informática debe auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

5.2.6 El Encargado de Informática debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

5.2.7 Es responsabilidad del El Encargado de Informática revisar periódicamente las bitácoras de los sistemas a su cargo.
5.2.8 El Encargado de Informática reportará a la Gerencia los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.
5.2.9 En caso de daño leve en el equipo, el personal de soporte técnico deberá repararlo o de no lograrlo notificará al usuario para que tome las medidas correspondientes, si el equipo se manda a reparación.
5.2.10 La instalación de Software específico deberá ser realizada en conjunto y común acuerdo del usuario que lo solicite y el encargado de Informática.

5.3 Renovación de Equipo
5.3.1 Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo para programar con anticipación su renovación de manera de no afectar las actividades de La Entidad.
5.3.2 Para la adquisición de equipo de cómputo se deberán solicitar al menos tres cotizaciones o según disposiciones legales vigentes.
5.3.3 Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar el requerimiento con las especificaciones técnicas apoyándose con la asesoría del Encargado de Informática a fin de que se seleccione el equipo adecuado. Sin el Visto Bueno del El Encargado de Informática no podrá liberarse una requisición de compra de equipo.

CAPÍTULO 6
POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DE SERVICIOS DE RED

6.1 Servicios en las Oficinas Centrales y Agencias

6.1.1 La Gerencia definirán y autorizara los servicios de Internet a ofrecer a los usuarios y se coordinará con el Encargado de Informática para su otorgamiento y configuración.

6.1.2 El Encargado de Informática es el responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

6.1.3 No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la empresa.

6.1.4 La Gerencia deberá notificar al Encargado de Informática cuando un usuario deje de prestar sus servicios a la empresa.

6.1.5 El Encargado de Informática realizará las siguientes actividades en los servidores de la empresa:

- Respaldo de información siguiente: base de datos de afiliación y prestamos
- Revisión de bitácoras y reporte de cualquier eventualidad de la RED.
- Implementar de forma inmediata las recomendaciones de seguridad proporcionados y reportar a la Gerencia posibles faltas a las políticas de seguridad en cómputo.
- Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- Calendarizar y organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

6.2 Uso de los Servicios de red por los usuarios

6.2.1 El Encargado de Informática será el responsable de definir y asignar la contraseña del usuario de acuerdo a la estructura definida. El usuario será responsable de la confidencialidad de la misma.

6.2.2 El Encargado de Informática cuando lo considere necesario o a solicitud del usuario deberá renovar las contraseñas, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

- Cuando ésta sea una contraseña débil o de fácil acceso.
- Cuando crea que ha sido violada la contraseña de alguna manera.

6.2.3 El usuario deberá notificar al Encargado de Informática en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

6.2.4 Si un usuario viola las políticas de uso de los servidores, El Encargado de Informática notificará a la gerencia para que imponga las sanciones pertinentes

CAPÍTULO 7
POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DEL ANTIVIRUS INSTITUCIONAL

7.1 Antivirus de la Red

7.1.1 Las Soluciones Antivirus deberán ser implementados y administrados para la prevención y la corrección de contagio por virus informáticos de la RED

7.1.2 Todos los equipos de cómputo deberán tener instalada la Solución Antivirus.

7.1.3 Periódicamente se hará el rastreo en los equipos de cómputo, y se realizará la actualización de las firmas antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

7.2 Políticas antivirus.

7.2.1 El Encargado de Informática será el responsable de:

- Implementar la Solución Antivirus en las computadoras de la entidad.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.
- Configurar el analizador de red para la detección de virus.

7.2.2 El administrador de la Red aislará el equipo o red, notificando a la Gerencia correspondiente, en las condiciones siguientes:

- Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros Equipos y redes.
- Si el usuario viola las políticas antivirus.

7.2.3 Cada vez que los usuarios requieran hacer uso de discos, USB's, discos duros extraíbles o cualquier medio de almacenamiento externo, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.

7.2.4 En caso de contingencia con virus El Encargado de Informática deberá seguir el procedimiento adecuado para ello.

7.3 Uso del Antivirus por los usuarios

7.3.1 El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

7.3.2 Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.

7.2.3 El usuario que cuente con una computadora con recursos limitados, contará con la versión ligera de la Solución Antivirus Institucional.

7.2.4 El usuario deberá comunicarse con El Encargado de Informática en caso de problemas de virus para buscar la solución.

7.2.5 El usuario será notificado por El Encargado de Informática en los siguientes casos:

- Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
- Cuando sus archivos resulten con daños irreparables por causa de virus.
- Cuando viole las políticas antivirus.

Dado en la ciudad de San Salvador, veintiséis de febrero del año dos mil trece.

REFORMAS.

(1) **ACTA CD 07/2018.** ACUERDA: Reformase el numeral 3.4.11 del Manual sobre Políticas y Procedimientos de Controles Generales de Información, aprobado en Acta CD 36/2013 de fecha veintiséis de septiembre del año dos mil trece, en el sentido que la cuenta de correo electrónico institucional deberá estar conformado por el nombre del puesto de trabajo, quedando la sintaxis de la cuenta de correo de la siguiente manera: nombredelpuesto@camudasal.gob.sv.-

CAJA MUTUAL DEL ABOGADO DE EL SALVADOR – CAMUDASAL – San Salvador