Manual de Políticas y Estándares de Seguridad Informática

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DE INFORMÁTICA.

Versión: 01	*Código:MPSI01*	*Fecha: Noviembre 2017*	*N.º Páginas:*

Rubro	Nombre	Cargo	Firma
Revisado Por:	Ing. Ausel Garcia	Gerente General	
Aprobado Por:	Concejo Municipal		

INDICE

INTRODUCCIÓN

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la Municipalidad una cultura de calidad operando en una forma confiable, además de garantizar el buen funcionamiento de los procesos, para contribuir con su eficiencia, optimizar los sistemas internos y garantizar la calidad en la gestión, con el objetivo de garantizar la seguridad de los datos y equipos.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Con este manual, se pretende trazar los lineamientos bajo la responsabilidad del área de Informática, como de los usuarios que hacen uso de la tecnología, a fin de que toda administración en este contexto se realice de una manera clara, precisa, transparente y lo más real posible, donde se respeten los principios éticos que dentro del marco normativo aceptado por la sociedad, produciendo así una escala de valores de hechos y formas de comunicación dentro de la Municipalidad.

1. DISPOSICIONES GENERALES

1.1. Ámbito de aplicación y fines

Las políticas de seguridad en informática tienen por objeto establecer las medidas de índole técnicas de organización, necesarias para garantizar la seguridad de las tecnologías de información y comunicaciones (Equipo de cómputo, sistema de información, redes telemáticas y datos) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de la institución, facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

1.2. Frecuencias de evaluación de las políticas

Las políticas del presente documento tendrán una revisión periódica, con una frecuencia anual para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias del personal de informática o gerencias y jefaturas de la institución.

1.3. Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC´s) en la Institución.

1.4. Autorización

El Manual de Políticas y Estándares de Seguridad Informática, es aprobado, previa revisión y verificación del Gerente General y autorizado por el Concejo Municipal.

1.5. Definiciones

Base de Datos: colección de Archivos interrelacionados

Antivirus: Pieza de software especializado en la detección y eliminación virus computacionales

Centro de cómputo . Salas de computo y/o salas de procesamiento de información que cuenten con equipamiento de cómputo.

Centro de Operaciones de red. Es el área que se encarga del funcionamiento y operación de las tecnologías de información y comunicaciones de la Alcaldía de Soyapango.

Centro de Telecomunicaciones: Espacio designado en la dependencia a los equipos de telecomunicaciones y servidores.

Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

DBA: Administrador de Base de Datos, del inglés Data Base Administrator.

Recursos Informáticos: Cualquier componente físico o lógico de un sistema de información.

Telemática: Conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática ofreciendo posibilidades de comunicación e información.

TIC: Tecnología de información y Comunicaciones, conjunto de teorías y de técnicas que permiten el aprovechamiento practico de la Información.

Usuario: Cualquier persona que haga uso de los servicios de las tecnologías de Información proporcionadas por el Departamento de Informática, tales como: equipos de cómputo, sistemas de información, redes telemáticas.

Virus Informático: Programa ejecutable, pieza de código con habilidades de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, y causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de computo.

Windows: Está diseñado para ser un sistema operativo directo y fácil de usar. Desde su

innovador y atractivo diseño visual hasta asistentes más intuitivos, hará que la experiencia en su PC sea la más natural posible. Ahora podrá encontrar todo lo que necesita con facilidad, gracias a funciones como el Asistente de Búsqueda o el uso de agrupamiento de archivos y carpetas para organizar sus archivos y carpetas de forma que tengan sentido para usted. Encontrar su información financiera, acceder a su información personal que son tareas muy fáciles de manejar.

Linux: Es un sistema operativo de código abierto, lo que permite hacerle cambios y personalizarlo es por eso que los programadores están escogiendo este sistema operativo.

Debian: Es conocido por adhesión a las filosofías de software libre y por su abundancia de opciones, su actual versión incluye mas de 18 mil paquetes de software, por sus estrictas políticas con respecto a sus paquetes y la calidad de sus lanzamientos. Estas prácticas permiten fáciles actualizaciones entre lanzamientos y una instalación y administración sencilla de paquetes.

Unix: Es una familia de sistemas operativos tanto para ordenadores personales como para servidores. Soporta gran número de usuarios y posibilita la ejecución de distintas tareas de forma simultánea (multiusuario y multitarea). Su facilidad de adaptación a distintas plataformas y la portabilidad de las aplicaciones (está escrito en lenguaje C) que ofrece hacen que se extienda rápidamente.

2. POLÍTICAS DE SEGURIDAD INSTITUCIONAL

POLÍTICA: Altas, Bajas y Cambios de usuarios en la red de la institución y las restricciones de acceso a las diferentes aplicaciones.

Toda persona que ingresa como usuario nuevo a la institución para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Procedimientos de Seguridad Informática para Usuarios.

2.1. Usuarios Nuevos

Todo personal que ingrese como administrativo para manejar equipos de cómputo y hacer uso de equipos informáticos, deberá ser notificado a la gerencia de informática, para asignarle su cuenta de sesión de usuario y permisos correspondientes o en caso de retiro del funcionario o empleado, anular y cancelar los permisos otorgados como usuario informático.

2.2. Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

2.3. Capacitación en seguridad informática

Todo empleado municipal o funcionario nuevo deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, Manual de Usuarios de Sistema integrado de su área, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

2.4. Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta institución, o de que se le declare culpable de un delito informático.

2.5. Control del Equipo Informático

La Gerencia de Informática llevará un control total y sistematizado de los recursos de cómputo y tecnológicos de la municipalidad, en donde cada gerencia o jefatura solicitara su asignación de código de inventario del equipo ya sea este donado o adquisición directa.

3. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Política: Para el acceso a los sitios y áreas restringidas (Centro de Datos) se debe notificar a la Gerencia de Informática para la autorización correspondiente, y así proteger la información y los bienes informáticos.

3.1. Protección de la información y de los bienes informáticos

- ➔ El usuario o funcionario deberán reportar de forma inmediata a la Gerencia de Informática cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
- ➔ El usuario o funcionario tienen la obligación de proteger el equipo que se encuentren bajo su responsabilidad ademas de los medios magnéticos que estén bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- ➔ Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información confidencial de la municipalidad que se encuentre almacenada en los equipos de cómputo que tengan asignados.

3.2. Acceso Físico

➔ Todos los Equipos de comunicación de datos y servidores estarán debidamente protegidos con la infraestructura apropiada y centralizados dentro del Centro de datos de manera que sea restringido para todos los usuarios.

➔ Las visitas internas o externas al Centro de Datos Institucional son restringidos para personal de otras áreas, solo ingresan acompañadas por personal de informática con previa notificación.

➔ Los equipos de cómputo de la Municipalidad deberán ser utilizados única y exclusivamente por el usuario a quién estén asignados.

➔ Cualquier persona que tenga acceso a las instalaciones de la Municipalidad, deberá registrar la entrada de su equipo y herramientas que no sean propiedad de la entidad, y notificar su visita a la unidad que se dirige. En caso contrario deberá tramitar la autorización de salida posterior correspondiente en la unidad donde ingresan con el equipo.

➔ Los equipos Informáticos y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de la Municipalidad únicamente con la autorización de salida de la unidad proveniente, donde especificara hacia donde se traslada el equipo.

3.3. Protección Física y Ubicación de los Equipos

Las puertas de acceso a los centros de datos deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.

El centro de datos Municipal debe ser un área restringida, además de :

- Recibir limpieza al menos una vez por semana, mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Contar por lo menos con dos extinguidores de incendio adecuado y cercano al centro

de telecomunicaciones.

- Contar con protectores eléctricos y reguladores de voltaje
- Contar con 2 aires acondicionados. Mantener la temperatura a 19 grados centrados.
- Asignar un técnico para que realice un control diario de temperatura y relevo de aires acondicionados y llevar un registro de fallas.
- Respaldo de energía redundante.
- El centro de Datos central y puntos de enlace deberá seguir los estándares vigentes para una protección adecuada de los equipos de telecomunicaciones, servidores y gabinete, estos deben estar en ambientes acondicionados y con protecciones en instalaciones eléctricas.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas, los equipos de aires acondicionados de los centros de telecomunicaciones internos y externos deberán recibir mantenimientos trimestrales con el fin de determinar la efectividad del sistema.

➔ La unidad de Contabilidad junto con el personal de Control y Activos Fijos será la encargada de generar el resguardo y recabar la firma del usuario como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por su jefatura.

➔Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Unidad de Informática, en caso de requerir este servicio deberá solicitarlo a la unidad de informática.

➔El usuario debe mantener el equipo informático en un lugar limpio y sin humedad, además de mantener libre el CPU sin objetos encima, ni papeles, también asegurarse de no poner botellas con agua cerca de los equipos, por derrames de líquidos que puedan dañarlos o hacer corto circuitos.

➔ El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar su reubicación de cables con el personal de la Unidad de Informática.

➔ Cuando se requiera realizar cambios simples/múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación a la unidad de Informática a través de un plan detallado.

➔Queda terminantemente prohibido que el usuario o funcionario de cada unidad Municipal abra o destape los equipos de cómputo, sino es autorizado por informática.

3.4. Respaldos de Información

La unidad informática realiza diariamente las copias de respaldo de Las Bases de Datos del sistema de Información Municipal, aplicativos e imágenes que se procesan en los servidores de producción en forma automática y manual.

➔ Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permita tener contingencia y continuidad de negocio. Además de generar copias en Medios magnéticos: DVD, Discos duros y en server de respaldo interno.

➔Los servidores de contingencia de Bases de Datos y aplicaciones que estén alojados externo a la municipalidad, en centros de DATA para resguardo de información, donde el único que tendrá acceso es el jefe de la unidad informática para su verificación y envío de las copias de respaldos.

➔Los servidores de hosting estarán alojados fuera de la municipalidad, con instituciones que

proveen el servicio de Internet.

➔ Dentro de este backup, no se incluirá información personal del usuario solamente la relacionada a la Municipalidad, la unidad de Informática verificará periódicamente lo guardado y borrará archivos que no correspondan a funciones de la municipalidad.

➔ Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros, dependiendo de la importancia y frecuencia de cambio; y sera responsabilidad absoluta de los usuarios resguardar su información.

➔ Los Técnicos de la unidad de informática no podrán remover información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los equipos o sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

➔ A cada usuario referido a la unidad de Informática le será creada una carpeta personal con acceso restringido, dentro del servidor de uso compartido correspondiente a carpetas de su unidad.

➔ El backup del Centro de Monitoreo, sera resguardado temporalmente de 6 a 8 meses en Discos duros de 2TB y discos externos 4TB.

3.5. Recursos de Usuarios

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores de La Municipalidad.

➔ Es responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas y en telecomunicaciones que utiliza, a fin de evitar riesgos por mal

uso y aprovechar al máximo las mismas.

➔ Los usuarios deberán almacenar su información únicamente en la partición del disco duro diferente, destinada para archivos de programas y sistemas operativos, generalmente c:\ Documentos, o escritorio .

➔ El uso de la carpeta compartida (10.10.1.5) es exclusivo para transferencia de información no para almacenamiento de estos, ni uso de resguardo de información personal o contenido de imágenes, música. Etc.

➔Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y Red de La Municipalidad, de acuerdo con las políticas que en este documento se mencionan.

➔ El Uso Apropiado de los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

➔ El usuario no debe tener acceso para Albergar datos (fotografías, musicas, libros, vídeos) de carácter personal en las unidades locales de disco de los computadores de trabajo, ni permisos para descarga de pornografía que sea almacenada en el disco de compartida de datos.

➔ Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Unidad de Informática:

- Instalar software en cualquier equipo de la Municipalidad;
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la

Municipalidad;

- Modificar, revisar, transformar o adaptar cualquier software propiedad de la Municipalidad
- Descompilar o realizar ingeniería inversa en cualquier software de la Municipalidad.

3.6. Uso de dispositivos extraíbles

➔La Unidad Informática, velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

➔ Cada Jefe de Área o dependencia debe reportar a la Unidad de Informática el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.

➔ El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen, por lo cual es restringido su uso y el usuario que tengan asignados estos tipos de dispositivos serán responsables del buen uso de ellos.

➔Toda Gerencia o Jefatura deberá solicitar a la unidad informática el acceso a uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

3.7. Instalaciones de equipos de cómputo

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

➔ Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.

➔ El Área de Informática, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.

➔ Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

➔ Las instalaciones se apegarán estrictamente a los requerimientos de los equipos,cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

➔ Para instalaciones de red interna, El usuario deberá garantizar las conexiones eléctricas en la ubicación requerida de su escritorio, caso contrario deberá colocarse en donde exista el toma mas cercano.

3.8. Renovación de equipos

Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

➔ Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para mejora del desempeño de sus actividades, estas deberán realizar una consulta a la unidad de Informativa a fin de que se seleccione el equipo adecuado.

➔ Una vez pasado los 5 o 10 años de la vida útil del equipo se deberán realizar los procedimientos de gestión de la renovación del equipo.

3.9. Mantenimiento de los Equipos Informáticos

La Unidad de Informática junto al Personal Técnico son los autorizados de llevar a cabo los servicios y reparaciones al equipo informático.

➔ El Mantenimiento preventivo es aplicado dos veces al año y el correctivo de forma inmediata durante la persistencia de la falla en el equipo.

➔ Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación, en caso que se tenga que formatear, el Técnico tiene la obligación de hacer Backup del equipo y recuperar nuevamente el contenido en la PC del usuario, en casos de perdidas irrecuperables de información por la falla del equipo que no lo permite se le notifica al usuario antes de proceder con su autorización.

3.10. Perdida o Transferencia de los Equipos Informáticos

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 usuario deberá dar aviso de inmediato a la Gerencia de Informática cuando se de la desaparición, robo o extravío del equipo de cómputo, equipos de telecomunicación o accesorios bajo su responsabilidad.

4. POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED

Política: La Red de datos de la municipalidad, tiene como propósito principal servir en la comunicación de datos e intercambio de información, dentro de la institución entre varios departamentos internos y externos.

4.1. Red de Datos Institucional

Nadie deberá copiar, alterar, o destruir la información que reside en los equipos de cómputo o servidores sin la debida autorización para hacerlo.

- ➔ La responsabilidad de la administración y mantenimiento de la red compete directamente a la unidad de Informática.

- ➔ 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 autoridades correspondientes.

- ➔ Las cuentas de Ingreso a los sistemas y los recursos de cómputo serán administradas directamente por la unidad de Informática en coordinación con las diferentes gerencias y jefaturas respectivas, y se usarán exclusivamente para actividades relacionadas con la Institución.
- ➔ Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos de usuarios.

- ➔ Cuando se detecte un uso no aceptable de la red, se bloqueará la entrada temporal o permanentemente del usuario o red involucrado y se informará a su respectiva jefatura. La reconexión se hará en cuanto a solicitud de la jefatura respectiva.

4.2. Los Servidores de Producción y Pruebas

La unidad de Informática, tiene responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

➔ La instalación y/o configuración de todo servidor conectado a la Red, deberá ser solicitada a través de memorándum Interno al departamento de Informática.

➔ Durante la configuración de un servidor los encargados del departamento de Informática deben normar 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.

➔ Los servidores que proporcionan servicios a través de la Red e Internet deberán cumplir con lo siguiente:

a) Funcionar 24 horas x 8 días los 365 días del año
b) Recibir mantenimiento preventivo y correctivo
c) Recibir mantenimiento mensual que incluya depuración de bitácoras
d Recibir mantenimiento semestral que incluya la revisión de su configuración
e) Ser monitoreado por el Departamento de Informática del Área de Soporte Técnico.

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

a) Diariamente, información critica (base de datos, imágenes)
b) Semanalmente, los correos y los documentos Web
c) Mensualmente, configuración de servicios y bitácoras.

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

a) Acceso restringido
b) Temperatura adecuada al equipo
c) Protección contra descargas eléctricas
d) Mobiliario adecuado que garantice la seguridad de los equipos

4.3. Cuentas de Acceso Institucionales (correo, Internet, SIMUS)

La unidad de Informática se encarga de crear las cuentas a los usuarios para el uso de correo electrónico, Internet y SIMUS en los servidores que administra.

➔ Para efecto de asignarle su cuenta de correo, Internet y SIMUS el usuario deberá llenar formulario de solicitud, que será autorizado por su jefe inmediato, donde asignará los privilegios que tendrá para el manejo de aplicativos y entregarlo al departamento de Informática, con su respectiva firma. La cuenta deberá estar conformada por un nombre de usuario y su password asignada con máximo de 8 caracteres y no deberá contener alias.

➔ La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada. En caso de olvido de la contraseña por parte del usuario, deberá notificar a la unidad de Informática para formatearla y asignarle su nueva contraseña.

➔ Las cuentas de usuarios a los sistemas municipales serán solicitados por las unidades que tienen módulos asignados en sus operaciones diarias, con sus respectivos detalles de acceso a las funcionalidades, el cual se les genera su perfil de USUARIO Y CONTRASEÑAS.

➔ La Unidad de Informática debe cancelar o suspender las cuentas de los usuarios previa notificación o cuando en su monitoreo encuentra anomalías del uso del recurso de acuerdo a los siguientes casos:

a) Si la cuenta no se esta utilizando con fines institucionales
b) Si pone en peligro el buen funcionamiento de los sistemas
c) Si se sospecha de algún intruso utilizando una cuenta ajena.
d) Si la cuenta no es objeto de uso continuo para la funcionalidad de sus tareas.

4.4. Sistemas Institucionales de Información

El departamento de Informática, debe auditar periódicamente los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no validas o permisos extras que pongan en riesgo la seguridad de la información.

➔ El analista y Programador tendrán acceso a la información de la Base de Datos únicamente para:

a) La realización de los respaldos del sistema.

b) Solucionar problemas de datos erróneos ingresados por usuarios.

c) Diagnostico o monitoreo.

d) Realizara eliminaciones de datos duplicados, con autorización de su jefe.

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

4.5. Uso de Antivirus Institucional

Deberán ser utilizadas en la implementación y administración de la Seguridad Informática.

➔ Todos los equipos de cómputo Municipal deberán estar conectados en la consola del server del NOD 32 e instala la aplicación en cada terminal, la unidad de informática verificara la frecuencia de actualización del antivirus.

➔ Periódicamente se hará el rastreo en los equipos de cómputo por la unidad de Informática y se realizará la actualización de las firmas proporcionadas.

4.6. Uso de Antivirus por los usuarios

El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un

riesgo de seguridad ante el peligro de virus.

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

➔ El usuario que cuente con una computadora con recursos limitados, contara con la ligera de la Solución Antivirus Institucional.

➔ El usuario deberá comunicarse con la unidad de Informática en caso que su equipo presente amenaza de virus ingresado.

➔ El usuario será notificado por la unidad de Informática en los siguientes casos:

a) Cuando sea desconectado de la Red con el fin de evitar la propagación del virus a otros usuarios.
b) Cuando sus archivos resulten con daños irreparables por causa de virus.
c) Cuando viole las políticas de seguridad.

5. *POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO*

Política: Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la Municipalidad. De igual forma, deberán proteger la información reservada o confidencial, almacenada o transmitida, ya sea dentro de la red interna Municipal o hacia redes externas como Internet.

5.1. Uso de Internet

Establecer políticas de seguridad que garantizan la navegación segura y el uso adecuado de

la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

➔ La asignación del servicio de internet, deberá solicitarse por escrito en memorándum o formulario para crear usuarios y asignar servicios, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

➔ No se permite la navegación a sitios con contenidos peligroso para la Municipalidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la unidad de informática. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del jefe de cada unidad, si las funciones laborales le exigen este contenido informativo.

➔ La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

➔ 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 Municipal y no para propósitos personales.

➔ Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea

son:

NIVEL 1: FULL: Acceso Sin restricciones, búsqueda de todas las paginas WEB, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Gerencias y Jefaturas: Acceso sin restricciones a WEB, restringido a vídeos de Youtube, contenido para descargas y redes sociales.

NIVEL 3: Jóvenes con todo: Acceso sin restricciones a WEB,

NIVEL 4: SAFIM: Acceso sin restricciones a WEB, restringido a vídeos de Youtube, descargas y redes sociales.

NIVEL 5: Yo me Animo: Acceso sin restricciones a WEB, restringido a vídeos de Youtube, juegos, Acceso a redes sociales.

NIVEL 6: Intermedio: 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 7: Correo sin Facebook: Internet restringido y sin mensajería instantánea: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación

NIVEL 8: Restringido: El usuario tendrá acceso a la WEB y navegación ilimitada, sin servicios de mensajería instantánea, vídeos y juegos.

5.3. Uso de correo Electrónico Institucional

➔ 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 la institución, tales como: cadenas, publicidad y propaganda comercial, política, social, etcétera.

➔ Permite a los usuarios de la municipalidad, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones, con el dominio propio de la municipalidad. “alcaldiadesoyapango.gob.sv”

➔ Cuando un funcionario, usuario o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de La Municipalidad, su cuenta de correo será desactivada.

➔ El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la Municipalidad. Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo las áreas de Recursos Humanos y de Contratación son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas.

➔ Las cuentas de correo electrónico son propiedad la Municipalidad, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la Municipalidad, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función que desempeñan.

ANEXO: RECOMENDACIONES DE USO

PARA EL EQUIPO MULTIMEDIA Y EQUIPO DE COMPUTO DE MISIÓN CRÍTICA.

1. Usarse en áreas con aire acondicionado
2. Conectarse a tomas de corrientes regulados, si están disponibles
3. Mantenerse alejados de alimentos y bebidas
4. NO forzar las conexiones de los dispositivos de los equipos (estos solo pueden conectarse de una forma)
5. Ubicar los equipos de tal forma que el calor generado por estos indica los equipos de cómputo.
6. NO mover, no golpear los equipos cuando están encendidos.
7. Poner los equipos en modo de reposo (stand-by) durante al menos 5 minutos antes de apagarlo de manera definitiva.
8. Al terminar, enrollar los cables y acomodarlos para un transporte seguro. Sin embargo, los cables no deben enrollarse con radios de cobertura muy pequeños, ya que pueden fracturarse.
9. NO colocar los proyectores o cañones sobre computadoras portátiles, ya que la pantalla liquida puede dañarse.

PROTECCIÓN ELÉCTRICA EN INSTALACIÓN DE SISTEMA DE COMPUTO Y COMUNICACIÓN.

1. Captura la descarga atmosférica en un punto designado
2. Proteger contra circuitos de potencia
3. Proteger contra transitorios entrantes por los circuitos de comunicación y datos.

EL INFRASCRITO SECRETARIO MUNICIPAL,----------

CERTIFICA: Que en el Acta Número **CUATRO**, Sesión Ordinaria, celebrada por el Concejo Municipal de esta ciudad, el día veintitrés de enero de 2018, se encuentra el **ACUERDO** que literalmente dice:**"""""ACUERDO NÚMERO DOS:** Presentados que han sido por el Gerente General y la Gerente de Informática de esta Institución, el Manual de Procedimientos de Informática, Plan de Contingencia de Informática y el Manual de Política de Seguridad de Informática, a efecto de generar la normativa que permita proteger los equipos informáticos, las Tecnologías de Información y los Sistemas Informáticos, que a su vez dichos Manuales serán un mecanismo, para establecer los casos de responsabilidad administrativa, en cuanto a los servidores públicos que tengan a su cargo, cuidado y custodia los equipos en referencia, según lo establecen las Normas Técnicas de Control Interno Específicas, el Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación, de las Entidades del Sector Público; en tal sentido solicitan aprobación y autorización de los manuales y Plan según detalle:

1. Manual de Procedimientos de Informática.
2. Plan de Contingencia de Informática.
3. Manual de Política de Seguridad de Informática.

Este Concejo **ACUERDA:** Tener por recibida la presentación de los Manuales y Plan antes detallados, presentados por los Funcionarios en referencia, en consecuencia se aprueban en todas y cada una de sus partes, para su respectiva aplicación Institucional, instruyendo a la Gerencia de Informática, para dar cumplimiento y seguimiento a la presente resolución. La votación del presente acuerdo queda unánime. **COMUNÍQUESE.**

ES CONFORME A SU ORIGINAL, CON EL CUAL SE CONFRONTÓ.

Alcaldía Municipal de Soyapango, a los veintiséis días del mes de enero del año dos mil dieciocho.

ALCALDIA MUNICIPAL DE SOYAPANGO. SECRETARIA. San Salvador, El Salvador, C.A.

Licdo. Santos Vidal Ascencio Bautista.
Secretario Municipal.