# Alcaldía Municipal
# Yoro, Yoro

Oficio No. SYS-MY-034-2019

Yoro, Yoro, 11 de diciembre de 19

**David Samuel Antunez**
OIP

Estimado,

Remito a usted en formato PDF el Reglamento de las "Políticas de Seguridad de las Tecnologías de Información y Comunicación de la Municipalidad de Yoro o PSTIC", para ser publicadas en el Portal Único de Transparencia. -

El documento PDF: Incluye la Portada de las PSTIC y la certificación del acta firmada por la honorable Secretaria Municipal.-

Sin otro particular

**Eduardo Santos**
Jefe de Sistemas e Informática

Cc: Archivo

REGLAMENTO

# POLÍTICAS DE SEGURIDAD

## De La Tecnologias De Informacion y Comunicacion.

PSTIC

CORPORACIÓN MUNICIPAL DE YORO

HONDURAS

# CERTIFICACION

La Suscrita Secretaria Municipal en uso de las facultades que la Ley le confiere por medio de la presente Certifica el punto **No.11.09** de Acta **No.39** de la sesión ordinaria celebrada por la Honorable Corporación Municipal el día viernes 08 de noviembre del año dos mil Diecinueve *Que* literalmente dice 1.....2.....3.....4.....5.....6.....7.....8.....9.....10.....11.09 El señor Eduardo Santos del Departamento de Sistemas e Informática dio a conocer lo siguiente ante la Corporación Municipal, el Manual de Normas y Políticas Informáticas, fundamentadas en ISO 17202.- La Honorable Corporación Municipal apruebo: Por unanimidad de votos el Reglamento de Políticas de Seguridad de las Tecnologías de Información y Comunicación y felicitan al señor Eduardo Santos por su trabajo.- Firma y sello Diana Patricia Urbina Soto, Alcalde Municipal, Boris Ernesto Ochoa Fernández, Vice Alcalde Municipal, Firma de los Regidores que asistieron a la sesión Wualdina Lizeth Núñez George, Rigoberto Zelaya Flores, José Guadalupe Almendarez Urbina, José Mauricio Rosales Cardoza, Héctor Orlando Cárcamo Cárcamo, Eruvin Saúl Collart Orellana, Marcia Argentina Alvarado Barahona- Firma y sello Carmen Isabel Pérez Montalván. - Secretaria Municipal.

Dado en la ciudad de Yoro Departamento de Yoro, a los once días del mes de diciembre del año dos mil diecinueve.

MUNICIPALIDAD DE YORO SECRETARIA MUNICIPAL YORO, YORO, C.A.

**CARMEN ISABEL PÉREZ M.**
**SECRETARIA MUNICIPAL**

# Políticas de Seguridad de las Tecnologías de Información y Comunicación de la Municipalidad de Yoro

## PSTIC de la Municipalidad de Yoro

Las Políticas de Seguridad de las Tecnologías de Información y Comunicación de la Municipalidad de Yoro, tienen como propósito generar un ambiente propicio donde cada empleado y abonado pueda sentirse seguro, evitar la pérdida de información por el mal uso u omisión de los respaldos informáticos.

Las PSTIC de la Municipalidad de Yoro fueron aprobadas en el Acta numero 39 numeral 11.09 de fecha 08 de Noviembre de 2019.

Departamento de Sistemas e Informática.
muniyoro@gmail.com

# Contenido

# I. Introducción

La información y los recursos informáticos son activos importantes y vitales de la Municipalidad de Yoro, por lo que las máximas autoridades y todos los empleados en cualquier nivel jerárquico, tienen el deber de custodiarlos, preservarlos, utilizarlos y mejorarlos. Esto implica que se deben tomar las acciones pertinentes para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos contra muchas clases de amenazas y riesgos, por lo que deben adoptarse y aplicarse medidas de seguridad, sin importar los medios en los cuales la información se genera y/o guarde: (en papel o en forma electrónica); como se procesa (computadoras personales, servidores, correo de voz, etc.) y cómo se transmite (en físico, correo electrónico, conversación telefónica, chat corporativo, etc.).

Cualquier imprudencia, violación o incumplimiento en materia de seguridad puede ocasionar a la MUNICIPALIDAD perjuicios de diversa índole y consideración. Es por ello que los Usuarios deben estar conscientes que la seguridad es asunto de todos y por tanto, debe conocer y respetar las políticas que la MUNICIPALIDAD adopte en esta materia.

# II. Objetivos

Objetivo General: Definir las Políticas de Seguridad de las Tecnologías de la Información y las Comunicaciones en la Municipalidad de Yoro, las cuales son el fundamento para poder obtener un control efectivo sobre la información, su resguardo y las actividades de los funcionarios y empleados de la Municipalidad que son realizadas a través de operaciones de computo o del uso de equipos y recursos informáticos, proveyendo la información necesaria para que permita a todos los funcionarios, corporativos, empleados, participantes, beneficiarios del sistema y otros actores vinculados a la Municipalidad, crear una **"Cultura de Seguridad y Control de la Información",** para que tomen conciencia de la necesidad imperativa de proteger la Información, el Hardware, el software y las redes de datos y comunicaciones de la Municipalidad.

Objetivos Específicos:

- Consolidar la seguridad de la información como tema estratégico.
- Planear el manejo de la seguridad de la información de manera efectiva.
- Minimizar los riesgos inherentes a la seguridad de la información generando una reacción oportuna a incidentes de seguridad.
- Mayor control de la información recibida y/o proporcionada a terceros y aumento de la confianza de los mismos.
- Mejorar la imagen Institucional.
- Mayor efectividad para la toma de decisiones.

## III. Alcance

Las Políticas de Seguridad de las Tecnologías de Información y Comunicación de la municipalidad de Yoro son de aplicables a la administración de:

LA INFORMACION: Datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc).

EL SOFTWARE: Conjunto de Sistemas Operacionales, programas, productos, aplicaciones y plataformas que utiliza la Municipalidad.

EL HARDWARE: Conjunto de equipos de cómputo, telecomunicaciones y redes que utiliza la Municipalidad.

## IV. Definiciones

Para efectos de la aplicación de las presentes normativas y con una perspectiva de la tecnología de información, deberán de considerarse las siguientes definiciones:

Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

Activos de Información: Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores, tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

**Configuración Lógica:** conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

**Copia de respaldo o backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

**Contenido:** Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

**Contraseñas:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos

**Cuenta de acceso:** Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

**Dispositivos/Periféricos:** Aparatos auxiliares e independientes conectados la computadora o la red.

**Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

**Espacio en disco duro:** Capacidad de almacenamiento de datos en la unidad de disco duro.

**Herramientas ofimáticas:** Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

**Información confidencial:** Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

**Información/Documento electrónico:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

**Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.

**Licencia de uso:** Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario(usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

**Log o Bitácora:** Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

**Mantenimiento lógico preventivo:** Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.

**Mantenimiento físico preventivo:** Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.

**Medios de almacenamiento extraíble:** Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, Compact Flash, Memory Stick).

**Plataforma web:** Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

**Propiedad intelectual:** Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.

**Recurso informático:** Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

**Red de datos:** Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

**Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.

**Servicio informático:** Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

**Servidor:** Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando.

**Sistema de información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

**Software antivirus:** Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.

**Software de gestión:** Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado de los proceso del negocio.

**Software malicioso:** Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.

**UPS:** Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

## V. Normativa Aplicable Relacionada

Las Políticas de Seguridad están enmarcadas en la Ley de Municipalidad y demás disposiciones vigentes que le son aplicables, tales como:

1. Ley de Municipalidades
2. Constitución de la Republica
3. Ley de Administración Publica
4. Ley de Acceso a la Información Publica

5. ACUERDO DMINISTRATIVO Nº. 027/2003 –Manual de Normas de Control Interno Capítulo V Normas Generales Sobre Información y Comunicación.
6. Normas contables, contraloras, nacionales e internaciones vigentes en lo que aplique a los Sistemas de Inforación, ejemplo: NIIF, NICS, Resoluciones de SEFIN, TSC, ONADICI etc.
7. Normas Generales de Control Interno emitidas por el TSC y ONADICI.

## VI. Responsabilidad

Las Políticas de Seguridad de las Tecnologías de Información y Comunicación de la Municipalidad de Yoro son de obligatoriedad de cada uno de los funcionarios y empleados des de la Municipalidad en cualquier nivel jerárquico, sean temporales, permanentes o de elección pública, definidos como los usuarios y administradores de la información y equipos informáticos, así como cualquier otro usuario que utilicen de una u otra forma los sistemas de información o las redes tecnológicas de la Municipalidad.

Las Políticas son aplicables a cada una de las áreas, departamentos, oficina o entidades de la Municipalidad de Yoro.

En ese contexto, existen distintos niveles de responsabilidad en el manejo y uso de la información:

ADMINISTRADOR DE SISTEMAS: Es el responsable técnicamente de la administración, disponibilidad, seguridad y operación de un determinado sistemas de información, en función de su responsabilidad Institucional.

CUSTODIOS: Se denomina así a las personas o áreas que proporcionan servicios, sin que necesariamente conozcan la información que custodian, solamente la procesan, gestionan su almacenamiento y la hacen accesible.

DUEÑO: Es generalmente el titular del área funcional de un sistema específico en particular, con la potestad para definir el alcance, la operatividad y las limitantes del mismo y de autorizar el acceso a la información.

USUARIO: Es aquella persona, empleada de la MUNICIPALIDAD, que crea, lee, introduce, cambia o actualiza la información almacenada en los Sistemas Informáticos de acuerdo con los privilegios que le son asignados. Para adquirir un perfil de usuario es necesario que el jefe inmediato llene la forma 0601.

El incumplimiento de las presentes Políticas de Seguridad dará lugar a la aplicación de las sanciones laborales establecidas de conformidad a la Ley de Carrera Administrativa Municipal,

Código de Trabajo, Reglamento Interno y demás disposiciones internas relacionadas, sin perjuicio de las acciones civiles o penales que en su caso, puedan resultar aplicables.

# VII. Políticas de Seguridad

## A. Competencias Departamento De Sistemas E Informática

Es competencia y obligación del departamento de Sistemas e Informática:

- Asistir al encargado de compras en lo concerniente a compras de computadoras nuevas o cualquier accesorio de las mismas.
- Crear nuevos programas que vengan a facilitar la sistematización y aplicación los nuevos cambios de la tecnología.
- Efectuar cambios en el sistema operativo de la Municipalidad ya sea para mejorar o agilizar la ejecución del mismo.
- Restringir el acceso a la base de datos.
- Darle mantenimiento a la red de computadoras para que el flujo de información sea eficiente y exacto.
- Restringir accesos por usuarios a la base de datos, habilitándole a cada empleado únicamente las ventanillas y programas que tengan que ver con sus funciones.
- Es el Departamento responsable del mantenimiento y buen funcionamiento del servidor o servidores que tenga la Municipalidad.
- Digitalizar la documentación como respaldo de la gestión municipal.
- Seguimiento y monitoreo para que los programas tengan datos actualizados en coordinación con los responsables del manejo de los módulos.
- Actualizar continuamente los registros de los procesos a su cargo.
- Proponer políticas y normativas informáticas a la Corporación.
- Establecer procesos de respaldo de información.
- Brindar apoyo a la unidad de Auditoria interna para realizar los procesos de auditoria.
- Velar por el cumplimiento de las políticas y normativas informáticas.

## B. Políticas De Seguridad De Aplicación General

### 1. De Los Usuarios

Los usuarios son responsables de cumplir con cada una de las políticas de la Municipalidad relacionadas a la Seguridad de la Información y Las Telecomunicaciones, y en particular:

I. Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la Información, Hardware y Software de la Municipalidad.
II. No divulgar por cualquier medio, información confidencial de la Municipalidad a personas no Autorizadas.
III. Responder por todas y cada una de las transacciones efectuadas en el software con su usuario y contraseña asignada.
IV. Proteger meticulosamente su contraseña y evitar que sea vista por otros usuarios en forma inadvertida.
V. No compartir o revelar su contraseña a otras personas empleados o ajenos a la Municipalidad.

### 2. Seguridad de Información Sensible, Reservada o Confidencial

I. Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que acceda o maneje directamente, especialmente si dicha información es clasificada como sensible, reservada o confidencial.
II. Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral en la Municipalidad de Yoro, no podrán facilitarla más que a aquellos otros empleados que necesiten conocerla para la misma finalidad y se abstendrá de usarla en beneficio propio o de terceros.
III. Los usuarios no podrán compartir con terceros la información relevante al patrimonio personal o familiar de los contribuyentes.
IV. El inciso III no se aplicara si se cuenta con Carta Poder debidamente autenticada por un Notario.
V. Es responsabilidad de los encargados de la administración de los archivos físicos, velar por la integridad de la información almacenada físicamente.

### 3. Uso de las Estaciones de Trabajo

I. El usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para los efectos de control de inventario. El Área responsable deberá mantener los registros de inventario debidamente actualizados.

II. Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales.

III. Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera de la Municipalidad sin el Visto Bueno del titular de la Oficina, Departamento de Sistemas e Informática y por el Departamento de Bienes y el traslado debe estar motivado por los intereses y objetivos de la Municipalidad.

IV. Se prohíbe instalar y utilizar en el hardware asignado para sus actividades laborales, software no autorizado. En los equipos de la Municipalidad solo podrá utilizarse software oficial y su instalación será exclusiva del Departamento de Sistemas e Informática.

V. Está prohibido modificar la configuración del hardware y software establecida por el Departamento de Sistemas e Informática. Tampoco está permitido hacer copias del software para fines personales.

VI. El usuario es responsable de salvar periódicamente la información de su equipo personal cuando esté utilizando el hardware para evitar que un corte de energía u otra falla del equipo, le haga perder la información de manera permanente.

VII. El usuario es responsable de apagar el hardware que tenga asignado cuando finalice su jornada laboral o se tenga que ausentar por más de una hora.

VIII. Es responsabilidad del Encargado de Recursos Humanos notificar al Departamento de Sistemas e Informática tan pronto un empleado termine su relación laboral con la Municipalidad de Yoro y Trabaje en su propio Hardware, para proceder a la eliminación de la información propiedad de la Municipalidad.

IX. El usuario es responsable de mantener organizada la información en el disco duro y conservar en el mismo únicamente los archivos que necesita para llevar a cabo sus labores. Los archivos de uso personal como música, fotografías, videos, juegos, etc. Están prohibidos y estarán bajo la responsabilidad del usuario los daños que causaren al equipo o información de la Municipalidad por no acatar esta disposición.

X. Se prohíbe el uso del hardware y software de la Municipalidad a terceros o personas extra164as al mismo, salvo autorización escrita del Alcalde Municipal o Gerente General.

XI. Es responsabilidad de los usuarios identificar y reportar a su Jefe inmediato, hardware y software no autorizado, así como la pérdida o robo de los mismos.

XII. Es Responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:

- No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
- No colocar objetos pesados encima del Hardware.

- Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc.
- No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.
- No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el Departamento de Sistemas e Informática.
- Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
- Conservar a los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.

4. Usuarios y Contraseñas

I. Es Responsabilidad del Departamento de Sistemas e Informática la administración general de los usuarios.
II. Se debe de asignar un nombre de usuario único y que se pueda identificar de forma explícita a quien pertenece dicho usuario.
III. Se debe de generar contraseñas robustas, las cuales, son confidenciales e intransferibles para garantizar su óptima identificación.
IV. Se prohíbe asignar códigos de identificación de usuario genérico o universal, tales como: muniyoro, municipalidadyoro, alcaldía, alcalde. Exceptuando los casos en que usuarios genéricos sean utilizados para la comunicación entre plataformas.
V. Se prohíbe asignar códigos de identificación de usuarios a personas que no sean empleados de la Municipalidad, a menos que estén debidamente autorizados, por el Alcalde Municipal o Gerente General.
VI. Ningún usuario o programa debe de utilizar las contraseñas de administrador de sistemas, salvo personal autorizado.
VII. El DSeI desactivara los Códigos de Identificación de usuario que no sean utilizados en un periodo de un mes.
VIII. Los códigos de Identificación de usuario que cumplan con un periodo de tres meses en estado de inactivos, deben de pasar al estado de Cancelado en el Sistemas.
IX. Los Códigos de Identificación de los empleados que sean recontratados, deben de utilizar el código de identificación anterior, firmando de nuevo la nota de reactivación y acta de compromiso.

X. Es responsabilidad del Departamento de Sistemas e Informática velar por el cambio de contraseña de todos los aplicativos, sistemas y plataformas según el estándar de noventa días calendarios.

XI. Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe de escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartida o revelarla a cualquier otra persona. El usuario que viole esta normativa será responsable directo por todos los daños y perjuicios que resulten de tal violación.

XII. Todo aplicativo debe de ser auditable, es decir, debe de permitir dejar rastro de todas las transacciones críticas generadas: bitácora (log) de transacciones y registros de entradas y salidas de usuario.

XIII. Ningún usuario puede tener más de un código de identificación de usuario para el acceso de la misma aplicación.

XIV. Es responsabilidad de Recursos Humanos que tan pronto como un empleado termine su relación laboral con la Municipalidad de Yoro, se proceda a realizar la cancelación de sus códigos de identificación de usuario y Contraseña, notificando al Departamento de Sistemas e Informática de tal cambio por escrito para hacer las gestiones necesarias de seguridad y de resguardo de la información propiedad de la Municipalidad.

XV. Es Responsabilidad del Departamento de Sistemas e Informática, realizar una revisión periódica de al menos cuatro veces al año, de los accesos asignados a los usuarios.

5. Política de Antivirus

Responsabilidades de los Usuarios

I. Mantener el Antivirus permanentemente activo para que vigile constantemente todas las operaciones realizadas en el Sistema. Está terminantemente prohibido al Usuario desactivar el Antivirus.

II. Dar aviso inmediato al Departamento de Sistemas e Informática y apagar el Hardware asignado inmediatamente que detecte la presencia de virus electrónico que no es eliminado por el antivirus.

III. Revisar con el Antivirus sus unidades de disco flexible, discos removibles o memorias USB (flash) antes de usarlas.

Prohibiciones:

IV. Está terminantemente prohibido al Usuario ejecutar los archivos si no provienen de una fuente reconocida y segura.

V. Queda terminantemente prohibido al Usuario compartir el disco duro del Hardware que tenga asignado, si necesita compartir alguna carpeta debe de obtener la autorización correspondiente y solo hacerlo al usuario destino.

6. Uso de Internet

I. Es responsabilidad del Usuario utilizar Internet únicamente con propósitos laborales. Queda terminantemente prohibido a los Usuarios el acceso, la transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, dato o material que viole estas Políticas, la Ley o los protocolos electrónicos.

II. Es responsabilidad del Usuario evitar la descarga de archivo desde el Internet. Ante de realizar una descarga desde Internet, el Usuario deberá solicitar al Departamento de Sistemas e Informática el software que requiere.

III. Queda terminantemente prohibido a los Usuarios el acceso a Internet por medio de dispositivos o servidores que no sean de la Municipalidad tales como Módems, USB, accesos inalámbricos o redes externas o por medio de otros proveedores cuando esté haciendo uso de la red de la Municipalidad.

IV. Es responsabilidad de los Usuarios desconectarse inmediatamente de las páginas de Internet que tenga contenido ofensivo, ya sea sexual, pornográfico, político, racista o de cualquier otro tipo.

V. Los usuarios que accidentalmente se conecten a estas páginas deberán informar a su jefe inmediato, quien deberá comunicarse con Jefe de Sistemas e Informática para bloquear estos accesos.

VI. Es responsabilidad del Jefe de Sistemas e Informática, autorizar o denegar el acceso a Internet, de forma temporal o permanente y acorde al perfil del cargo del solicitante. Dicho acceso deberá ser solicitado por medio del procedimiento correspondiente y se otorgara (si procede) previa aprobación del Gerente General.

## C. Política de Seguridad de Aplicación Específica

# Área de Sistemas

### 1. Seguridad de Servidores

I. Es responsabilidad del Jefe de Sistemas e Informática de la Municipalidad, administrar todos los servidores internos de la Municipalidad de Yoro, administrar el sistema de cada uno y contar como mínimo con la siguiente información relacionada:

- Nombre del Servidor

- Localización del Servidor
- Nombre del Administrador responsable
- Detalle especifico del Hardware
- Sistema Operativo y su versión
- Aplicaciones y Base de datos
- Función principal y/o uso
- Acuerdo de Mantenimiento (Plan detallado –Cronograma)

II. Es responsabilidad de cada encargado del servidor, que todos los servidores, así como su sistema operativo, tenga estándares de configuración de seguridad de documentos y aplicados de acuerdo al rol del servidor.

III. Es responsabilidad del Jefe de Sistemas e Informática, que las actualizaciones más recientes de seguridad sean instaladas en los servidores tan pronto como sea posible.

IV. Es responsabilidad del Jefe del Departamento de Sistemas e Informática, definir los procesos tecnológicos, mantenerlos actualizados y velar por su cumplimiento, para mantener los servidores protegidos físicamente en un ambiente con control de acceso y protección ambiental.

## 2. Seguridad de Equipos de Comunicación

I. Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, video seguridad y computo deben ser tratadas como Información Confidencial.

II. Es responsabilidad del Jefe de Sistemas e Informática de la Municipalidad, definir los procesos de su área, mantenerlos actualizados y velar por su cumplimiento, para que todos los recursos de red críticos como enlaces de comunicación, firewalls, servidores, centrales de conexión de la Municipalidad, son de acceso físico restringido.

III. Queda terminantemente prohibido que los empleados y funcionarios de la Municipalidad lleven a cabo algún tipo de instalación de líneas telefónicas digitales o análogas, canales de transmisión de datos, módems o cambiar su configuración esto es responsabilidad exclusiva del área de informática o de cualquier empresa que se haya contratado para tal fin, en cuyo caso será supervisado por el Departamento de Sistemas e Informática.

IV. Queda terminantemente prohibida la utilización de herramientas de monitoreo de red, esta activada esta restringida solo al departamento de Sistemas e Informática de la Municipalidad.

## 3. Acceso y Configuración de Remotos

I. Esta prohibido otorgar cuentas o acceso remoto a la red de la Municipalidad de yoro a menos que sea autorizado por el Jefe de Sistemas e Informática o Gerente General y solo a través de VPN's que cuenten con las medidas de seguridad adecuadas.

## 4. Seguridad en Redes Inalámbricas

I. Es responsabilidad del Jefe de Sistemas observar las siguientes prácticas en la administración de las redes inalámbricas:
   - Cambiar la contraseña asignada por el fabricante o de instalación.
   - Activar el filtro de direcciones MAC.
   - Restringir de acuerdo con lo establecido el número máximo de dispositivo que pueden conectarse.
   - Utilizar siempre protocolos de encriptación que estén de acuerdo con los estándares internacionales vigentes.
   - Proporcionar un entorno físicamente seguro a los puntos de acceso.
   - Utilizar IPSec, VPN, Firewalls y monitorear los accesos a los puntos de acceso.
   - Inhabilitar la emisión Broadcast del SSID.
   - Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos.

## 5. Centro de Datos, Sistemas y Telecomunicaciones

I. Los Centros de Datos, Oficinas de Sistemas y Área de Telecomunicaciones de la Municipalidad de Yoro están clasificadas como áreas de acceso restringido.

II. Es responsabilidad del Jefe de Sistemas e Informática de la Municipalidad de Yoro, asegurar que todos los recursos de computación y telecomunicaciones de la Municipalidad, reciban mantenimiento preventivo y/o correctivo.

III. Es responsabilidad del Jefe de Sistemas e Informática que los Centros de Datos, Oficinas de Sistemas y áreas de Telecomunicaciones de la Municipalidad cuenten con sistemas de control de acceso físico, que puedan ser auditados.

## 6. Respaldos

La Municipalidad deberá contar como mínimo con dos centros u oficinas diferentes, para el almacenamiento de respaldos.

I. Es responsabilidad del Jefe de Sistemas e Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los datos de producción independientemente del servidor en el Centro de Datos donde se encuentre , el que debe cumplir con las siguientes reglas:
   - Periodicidad: Diaria
   - Tipo de Respaldo: Total
   - Retención: 5 años
   - Custodia: En centro alterno de almacenamiento
   - Prueba de Recuperación: Cada seis meses