POLITICAS Y LINEAMIENTOS DE SEGURIDAD DE COMPUTO

TLX
CONSTRUIR Y CRECER JUNTOS
GOBIERNO DEL ESTADO DE TLAXCALA 2017-2021

ITIFE
INSTITUTO TLAXCALTECA
DE LA INFRAESTRUCTURA
FÍSICA EDUCATIVA

Contenido

Sección de políticas

Objetivo

Establecer los lineamientos sobre los cuales se debe conducir el personal que labora en El Instituto Tlaxcalteca de la Infraestructura Física Educativa sobre el uso de la infraestructura, recursos de cómputo y telecomunicaciones con los que se cuenta en dicha dependencia.

Metas

Contar con reglamentos necesarios que resguarden la integridad de los recursos informáticos, para su correcto uso y aprovechamiento, manteniendo un ambiente de control donde el riesgo se minimice y se cuente con una base normativa como respuesta a cualquier incidente.

Alcance

Establecer en el presente documento diversos lineamientos, los cuales deben ser acatados por todo el personal o usuario que haga uso de la infraestructura informática de El Instituto Tlaxcalteca de la Infraestructura Física Educativa de acuerdo con sus diversas actividades que desempeñe dentro del mismo.

Comité de tecnologías de la información y telecomunicaciones

Tiene como objetivo establecer las medidas conducentes a fin de que la información relevante que generen sea adecuada para la toma de decisiones y el logro de los objetivos, metas y programas institucionales, así como para cumplir con las distintas obligaciones a las que en materia de información están sujetas, en términos de las disposiciones legales y administrativas aplicables.

Oficina de informática

La oficina de informática es la encargada de definir y ejecutar diversas estrategias que ayuden a brindar seguridad en cómputo y de esa forma disminuir la cantidad y gravedad de problemas que pudiesen surgir dentro de ITIFE.

1. Políticas de seguridad física

Seguridad física hace mención a los controles y mecanismos de seguridad dentro y alrededor de las diversas oficinas o departamentos donde existan equipos de cómputo, implementados para proteger el hardware y medios de almacenamiento de datos.

Políticas

1.1. Al instalar los equipos de cómputo en las diversas oficinas o departamentos se debe verificar que sea un lugar apropiado alejado de diversos factores que puedan afectar la integridad de estos o infieran en su funcionamiento como son: polvo, temperaturas extremas, rayos solares, radiaciones eléctricas, suministros de agua o gas, etc.

1.2. Todos los servidores deberán encontrarse en lugares restringidos al acceso de cualquier usuario.

1.3. El lugar donde se instalen los servidores debe contar con una instalación eléctrica adecuada, así mismo debe contar con tierra física y sistemas de alimentación ininterrumpida o de emergencia, UPS (Uninterruptible Power Supply)

1.4. El área donde se encuentren los servidores debe encontrarse siempre limpio, no deben encontrarse objetos ajenos para el funcionamiento de estos, así como el lugar debe encontrarse a temperatura ambiente.

1.5. Se debe contar en cada oficina o departamento por lo menos con un extinguidor de incendio adecuado, de la misma forma debe existir personal capacitado para el uso correcto ante una contingencia.

1.6. En las diversas oficinas o departamentos que integran a ITIFE dónde existan equipos de cómputo deben encontrase a temperaturas ambientes con el fin de garantizar el correcto funcionamiento de estos, previniendo de esta forma el deterioro o mal funcionamiento.

1.7. Debe existir los controles necesarios para autorizar o no el acceso a las personas, cuales fuera su actividad o rol, a los equipos de cómputo.

1.8. Para hacer uso de los equipos de cómputo se prohíbe el estar ingiriendo cualquier alimento o bebida ya que esto pone en peligro la integridad de estos.

2. Políticas de reglamentos internos

Dentro de El Instituto Tlaxcalteca de la Infraestructura Física Educativa en sus diversas oficinas o departamentos existe diversidad de actividades, tareas y trabajos las cuales requieren de dinamismo y flexibilidad, por lo que las políticas presentadas a continuación tienen como objetivo el uso de reglamentos internos los cuales tienen que ser acatados por su personal.

2.1. Las oficinas o departamentos que requieran generar reglamentos internos o políticas de seguridad informática adicionales a las contenidas en este documento son libres de hacerlo, siempre y cuando se respeten y se consideren como prioritarias las mencionadas en este documento.

2.2. Los nuevos reglamentos o políticas de seguridad informática que se generen deben ir siempre a la par a las existentes persiguiendo siempre el mismo objetivo.

2.3. Se deben cuidar todos los aspectos de los nuevos reglamentos o políticas de seguridad informática que se generen para no caer en la contrariedad de algunos de los puntos existentes.

3. Políticas referentes al papel del administrador

El administrador de los equipos de cómputo o mejor llamado administrador de TI (Tecnologías de Información) es la persona con la autoridad y responsabilidad que se encarga de planificar, organizar, dirigir y controlar el recurso informático con la finalidad de asegurar la calidad y permanencia del servicio, así como la prestación del servicio ininterrumpido y seguro.

3.1. El cargo de administrador de sistemas que operará en la oficina de informática de ITIFE deberá ser asignado en base a diversos criterios algunos de estos son:

- Contar con un grado alto de experiencia en manejo de diversos sistemas computacionales.
- Contar con un perfil de responsabilidad y calidad en todas las actividades que desarrolla.
- Mantener un ambiente de respeto y tolerancia al personal que está involucrado en el desarrollo de su trabajo.
- Contar con una actitud de desempeño proactivo.
- Trabajo en equipo.
- Capacidad de reacción bajo presión.
- Facilidad en la resolución de problemas.
- Capacidad de reacción ante una emergencia.

3.2. El administrador debe tener conocimientos avanzados sobre temas de seguridad informática y redes.

3.3. El administrador debe tener conocimientos avanzados sobre el manejo y administración de diversos sistemas operativos como lo son Windows, Linux, entre otros.

4. Políticas de cuentas

Para acceder a una cuenta de un sistema informático todo usuario sea cual sea su rol, para desempeñar sus funciones necesita de un usuario y una contraseña, los cuales le brindaran un acceso permitido. Por lo cual se presentan diversas características que deben cumplir la creación de las mismas.

4.1. Las cuentas deben ser otorgadas exclusivamente a empleados de ITIFE, bajo los siguientes criterios:

- Ser empleados vigentes.
- Tener la autorización del jefe de oficina o departamento correspondiente.
- Justificar la necesidad de dicha cuenta para realizar una actividad en concreto.

4.2. Las contraseñas deben ser seguras, lo cual requiere cumplir con los siguientes criterios:

- Tener una longitud de ocho caracteres como mínimo, entre los cuales se debe incluir caracteres de tipo numérico y alfanumérico.
- Se deben diferenciar las mayúsculas y minúsculas.

4.3. Debe emplearse una contraseña distinta para cada cuenta que se genere.

4.4. La cuenta y contraseña que se asigne a cada usuario deber ser de carácter confidencial, es decir, el administrador debe hacer entrega al usuario de su cuenta y contraseña de manera personal, sin intermediarios, todo esto por motivos de seguridad.

4.5. Todas las acciones que se generen de cada una de las cuentas que se generen en los distintos sistemas informáticos de ITIFE es responsabilidad del usuario que se le asigno dicha cuenta.

4.6. Todas las cuentas que se generen son de uso personal e intransferibles.

4.7. El administrador debe contar con dos cuentas, una cuenta debe ser creada acorde a las actividades que este realizara, y la otra cuenta para dar solución a un problema que llegara a surgir en algún sistema informático y que en el estricto caso requiera el uso de la misma.

4.8. El usuario tiene todo el derecho de poder cambiar su contraseña siempre y cuando esta misma cumpla con todas las políticas establecidas en este documento.

4.9. Queda estrictamente prohibido el transferir o prestar las cuentas.

4.10. El administrador es el responsable de dar de baja las cuentas que no hayan sido utilizadas por más de tres meses.

5. Políticas de acceso remoto

Se considera acceso remoto a la conexión que se da entre equipos para realizar funciones en específico una de ellas puede ser la trasferencia de archivos o bien el control total de uno de los equipos entre muchas más. Por lo cual en el presente documento se procede a estipular cómo será el acceso a los sistemas de cómputo de ITIFE.

5.1. Todos los equipos de cómputo que proporcionen un servicio de acceso remoto, terminal remota, un formulario, de correo electrónico, o una aplicación que solicita o trasmite información sensible, deberán contar con aplicaciones que permitan una comunicación cifrada y segura.

5.2. Los sistemas deben tener la capacidad de almacenar el nombre de la cuenta, dirección IP, fecha, hora y cualquier otro dato que permita dar seguimiento sobre las acciones que se realizan.

6. Seguridad de información sensible

Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que acceda o maneje directamente, especialmente si dicha información ha sido clasificada como sensible. Dicho echo se estipulan los siguientes puntos.

6.1. Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral.

6.2. La información relativa a aportaciones, números de cuenta de banco, beneficiarios, estados financieros institucionales y de los participantes, y en general datos de los participantes, debe ser tratada como información confidencial.

6.3. La información relativa a los empleados debe ser tratada con especial cuidado como información confidencial sensible del recurso humano.

6.4. Es responsabilidad de los empleados garantizar que toda documentación en formato impreso, electrónico, etc., que contenga información sensitiva, una vez utilizada, o que no pueda ser entregada al propietario, sea archivada de manera segura o en su caso desechada.

6.5. Es responsabilidad de los encargados de archivos físicos, velar por la integridad de la información almacenada físicamente.

7. Políticas de uso adecuado

Estas políticas establecen lo que se considera un uso adecuado y correcto de los recursos de TI que brinda ITIFE.

Políticas:

Usuarios en general:

7.1. La instalación de programas o software, que se requiera debe ser solicitado al administrador de la oficina de informática.

7.2. El uso de los equipos de cómputo o impresoras es estrictamente con fines laborales, de esta forma al empleado que se le sorprenda haciendo distinto uso a los establecidos será acreedor a una sanción, la cual la determinara, el *administrador de la oficina de informática el cual se basara en las establecidas* en el apartado de sanciones y acorde a la magnitud del problema.

7.3. El uso a la infraestructura de red de ITIFE será con estrictamente con fines laborales.

7.4. Queda prohibido la descarga de programas o archivos que pongan en peligro la integridad de los equipos de cómputo.

7.5. Es responsabilidad de los usuarios desconectarse inmediatamente de páginas de Internet que tengan contenido ofensivo, ya sea sexual, pornográfico, político, racista o de cualquier otro tipo. Los usuarios que accidentalmente se conecten a estas páginas deberán informar al administrador de red de la oficina de informática, quien deberá bloquear estos accesos.

7.6. Se puede hacer uso de todo el software de aplicación que ya se encuentre instalado en los equipos de cómputo.

7.7. Se puede hacer uso de los sistemas de impresión o fotocopiado siempre y cuando sean con fines laborales.

7.8. Los equipos de cómputo que se encuentran en las distintas oficinas o departamentos de ITIFE, no podrán moverse o transferirse sin previa autorización de la oficina de recursos materiales o en su caso del encargado de la oficina de informática.

7.9. El envío y almacenamiento de todo tipo de información sensible o de carácter confidencial debe contar con las medidas apropiadas de seguridad para su protección, el usuario es responsable de habilitar estas medidas.

7.10. Es responsabilidad del dueño de la información, realizar y resguardar sus respaldos en los medios que considere pertinentes, protegiéndola de esta manera en contra de fallos que podrían traer como consecuencia la pérdida o corrupción de la misma.

7.11. El administrador de la oficina de informática es quien determinara la configuración a los equipos de cómputo (fondo de pantalla, restricciones a ciertos programas informáticos, etc.), las cuales tienen que ser respetadas por los usuarios.

8. Políticas de respaldos

Estas políticas especifican la responsabilidad que tiene cada usuario y el administrador de sistemas sobre el resguardo de toda la información que manejan.

Políticas

Usuarios en general:

8.1. Es responsabilidad de cada usuario mantener un respaldo de toda su información en un medio diferente al que se encuentra alojada, este medio puede ser una USB, disco duro, DVD o en servidores de almacenamiento web, todo con el fin de mantener segura la información ante posibles pérdidas.

Administradores:

8.2. El administrador del sistema es el responsable de realizar respaldos de la información y configuración constantemente en los sistemas a su cargo, verificando que se haya realizado correctamente y notificando previamente a los usuarios sobre la periodicidad de esta acción.

8.3. El administrador del sistema es el responsable de restaurar la información derivada de los respaldos que realiza, en caso de ser necesario.

8.4. En el momento en que la información almacenada sea obsoleta para la dependencia, dicha información debe destruirse del medio total y de forma permanentemente. Cada departamento determinará cuando la información es considerada obsoleta.

9. Políticas de correo electrónico

Establecen el uso adecuado del correo electrónico, así como las medidas de seguridad que tiene que acatar los usuarios.

9.1. Queda prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico.

9.2. Es responsabilidad del usuario el evitar incluir contenidos hostiles que molesten a los receptores del mismo, o que manchen la imagen de ITIFE, asimismo, es responsabilidad del usuario reportar a su jefe inmediato la recepción de este tipo de mensajes, quien a su vez deberá reportarla al jefe de la oficina de informática, para tomar las medidas correspondientes.

9.3. El uso del correo institucional de ITIFE es solo con fines laborales, el usuario que sea sorprendido haciendo mal uso del mismo será sancionado, acorde a la sanción correspondiente que designe el administrador de la oficina de informática el cual se basara de las estipuladas en el apartado de sanciones y a la magnitud del problema.

9.4. El jefe de cada oficina o departamento tiene la facultad de solicitar al administrador de la oficina de informática una cuenta de correo electrónico para que este mismo desempeñe sus actividades diarias.

9.5. Si se descubre a un usuario manteniendo dentro de su correo algún malware o cualquier tipo de amenaza a nuestros servidores de manera intencional este será sancionado, el administrador de la oficina de informática determinará la sanción correspondiente de acuerdo al apartado de sanciones y a la magnitud del problema el cual se basará en las establecidas en el apartado de sanciones y acorde a la magnitud del problema.

9.6. Los datos adjuntos recibidos en los correos pertenecientes a servidores de ITIFE serán filtrados para excluir extensiones como ".exe", ".bat", ".msi" y todas aquellas que el administrador considere de riesgo para la seguridad del sistema.

9.7. Los puntos de envío y recepción de correo institucional deben ser protegidos de accesos no autorizados, por la seguridad de la información.

10. Políticas de desarrollo de software

Las políticas aquí presentadas especifican los lineamientos para el desarrollo de aplicaciones de software.

10.1. El desarrollo de sistemas, herramientas y software en general cuyo propósito sea el de apoyar, facilitar y agilizar las actividades laborales o de investigación para ITIFE, así como los distintos proyectos en colaboración con alguna otra organización interna o externa, debe de seguir los lineamientos establecidos por ITIFE, en caso que estos no existan de manera particular para alguna tecnología, se debe de seguir las metodologías internas en cada dependencia considerando la compatibilidad entre sistemas.

10.2. Es necesario el desarrollo de documentación que permita dar seguimiento a las aplicaciones de software durante todo su ciclo de vida, siguiendo la metodología que la dependencia considere adecuada para dicho fin.

10.3. La elección de la tecnología de desarrollo y bases de datos debe ser realizada en referencia a la compatibilidad con los demás sistemas con los que la aplicación pueda interactuar.

10.4. Previa a la liberación de los sistemas de información debe de realizarse un análisis de seguridad en un ambiente de pruebas, corrigiendo la totalidad de los fallos que sean detectados.

11. Políticas de bitácoras del sistema.

Establecen los lineamientos bajo los cuales será registrada la actividad de los usuarios en los sistemas informáticos, así como la manera en que deben manejarse los registros y el propósito de los mismos.

11.1. El administrador del sistema debe contar con las herramientas necesarias que le ayuden a la detección de intrusos de host, verificadores de integridad, etc. Con el propósito de mantener evidencia ante incidentes.

11.2. Queda estrictamente prohibido el uso de algún software espía dentro de la infraestructura de red o de los equipos de cómputo todo esto para mantener segura la integridad de los datos que se manejan dentro de ITIFE.

11.3. El administrador de la oficina de informática es el responsable y único con la facultad de poder monitorear la red o equipos de cómputo todo esto para garantizar la integridad de la información que se maneja.

11.4. El administrador de la oficina de informática puede hacer uso de la información que se genera en las bitácoras, con el fin de poder deslindar responsabilidades ante cualquier incidente que pudiese llegar a presentarse.

12. Políticas de antivirus

Responsabilidades de los usuarios:

12.1. Utilizar el antivirus instalado por el administrador de la oficina de informática, el cual se ejecutará automáticamente una vez que se inicie el equipo de cómputo.

12.2. Mantener el antivirus permanentemente activo para que vigile constantemente todas las operaciones realizadas en el sistema. Está prohibido al usuario desactivar el antivirus, a excepción de que por una extrema razón se requiriera desactivar el mismo, se tendrá que notificar al administrador de la oficina de informática justificando la causa por el cual se requiere realizar dicha acción y de esta forma el administrador tome las medidas precautorias correspondientes.

12.3. Dar aviso inmediato a la oficina de Informática y apagar el equipo de cómputo asignado inmediatamente que detecte la presencia de un virus electrónico que no es eliminado por el antivirus, y de esta forma evitar daños mayores.

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

12.5. Mantener la base de datos del antivirus actualizada en caso de que no lo haga de manera automática, con el objetivo de obtener mejoras y estar mejor protegidos.

13. Políticas de impresoras

13.1. Se debe permitir la actualización del firmware de las impresoras esto con el fin de mejorar las funcionalidades o corregir posibles errores de su software.

13.2. Queda estrictamente prohibido la instalación de aplicaciones en las impresoras o para impresoras, ya que estas pueden ser potencialmente peligrosas y pueden ser usadas de forma maliciosa.

13.3. Es necesario avisar a la oficina de informática inmediatamente que la impresora muestre un código de error o muestre algún funcionamiento inusual, con la finalidad de evitar un daño mayor.

13.4. A las impresoras que puedan conectarse en red, se les debe de asignar una IP por el Administrador de la Oficina de informática y queda prohibido modificarla sin autorización.

13.5. Es importante utilizar un tipo de papel de impresión adecuado, con la finalidad de evitar inconvenientes como atasco de papel, mala calidad de impresión, desgaste innecesario en rodillos, etc.

13.6. Es importante usar tóner, tinta y cartuchos originales, para el buen uso del equipo y así obtener una mejor calidad de impresión.

13.7. Se debe tomar en cuenta el de brindar un mantenimiento preventivo a las impresoras por lo menos dos veces al año, con el objetivo de perdurar su vida útil.

14. Políticas de uso de direcciones IP

Políticas:

14.1. El jefe de la oficina de informática o administrador de red debe contar con un plano donde se muestre la distribución de las diversas cajas de conexión a internet existentes en las diversas oficinas o departamentos que conforman a ITIFE, así mismo un inventario, el cual contenga, las direcciones físicas tanto como el responsable del equipo de cómputo, además de otros datos que le resulten relevantes.

14.2. Ningún usuario final puede modificar o asignar una dirección IP al equipo de cómputo que tiene a su cargo.

14.3. Las subredes deben emplear rangos relacionados con la zona en la que se encuentren.

14.4. Se permiten rangos de direcciones privadas de la forma 192.168.2.X.

14.5. Las direcciones IP que pueden otorgarse son homologadas o privadas. Las homologadas sólo son otorgadas si se justifican su uso y disponibilidad.

14.6. El administrador de la red, podrá realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.

15. Políticas de sitios web

Las políticas aquí contenidas son lineamientos que se deben seguir para la operación de los diversos sitios Web o página de internet, de los cuales se hacen uso en los equipos de cómputo de ITIFE.

Políticas:

15.1. Es responsabilidad del administrador actualizar los certificados si es que se contara con alguno.

15.2. Los servicios que se prestan por medio de los servidores, deben contar solo con las herramientas y aplicaciones acorde a los servicios que estos prestan.

15.3. La configuración de los servidores es responsabilidad del encargado o administrador, como también son responsables del monitoreo, actualización, evaluación e instalación de parches de seguridad.

15.4. La creación de sitios web o repositorios de archivos creados en los servidores o equipos de ITIFE deber ser justificados, es decir deben ser solo con fines laborales.

15.5. El administrador o encargado de los servidores debe definir las medidas de seguridad necesarias para prevenir y minimizar el riesgo de ataques o infecciones por algún tipo de malware.

16. Políticas para redes inalámbricas

Políticas:

16.1. Queda prohibido la instalación de algún dispositivo inalámbrico de red sin la previa autorización del jefe de la oficina de informática de ITIFE.

16.2. Si se requiere una red para fines de experimentación de los diversos estándares y protocolos, esta tendrá que ser instalada de forma independiente y totalmente desconectada de la red de ITIFE.

16.3. El registro de una red inalámbrica se tiene que realizar ante el jefe de la oficina de informática.

16.4. Realizar el cambio de las claves por defecto cuando se instale el software del Punto de Acceso (Access Point) o AP.

16.5. La instalación y configuración de los puntos de acceso deberá ser realizada por personal capacitado con los conocimientos técnicos necesarios, además se deberán modificar los parámetros establecidos por el fabricante del dispositivo para evitar que cualquier individuo tenga acceso a los mismos.

16.6. El administrador es el encargado de cambiar el SSID que trae el equipo como predeterminado.

16.7. El manejo de las contraseñas es responsabilidad del administrador, encargado de la instalación de las actualizaciones, el uso de cifrado y de permitir el acceso de los usuarios al punto de acceso.

Sobre la seguridad de redes inalámbricas:

16.8. No deberán de existir redes inalámbricas que sean de tipo abiertas, es decir que no tengan un mecanismo de autenticación.

16.9. Las redes inalámbricas no podrán ser implementadas con direcciones IP homologadas.

16.10. Los "puntos de acceso" no podrán ser administrados por los clientes inalámbricos. Toda administración de los "puntos de acceso" se realizará por medio de la red cableada.

Sobre la conexión a redes inalámbricas:

16.11. Los usuarios no deben compartir su conexión a la red inalámbrica con ningún otro individuo.

16.12. Queda prohibido que el usuario que tenga una cuenta la pueda otorgar a otra persona para que acceda a la red.

16.13. Copias de programas y aplicaciones está prohibido a excepción de que exista el permiso correspondiente.

16.14. Las redes inalámbricas existentes en ITIFE deberán implementar como mínimo el método de cifrado de datos WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key).

17. Políticas de contratación y finalización de relaciones laborales de recursos humanos en sistemas informáticos

Políticas:

16.1 Queda excluido de ser nuevamente contratados como administradores de sistemas todos aquellos que hayan tenido incidentes graves acordes a las funciones que conlleva su rol.

16.2 El administrador o encargado de los sistemas de información deberá cambiar todas las contraseñas cuando un administrador deje de prestar sus servicios a ITIFE.

16.3 Todo personal que termine una relación laboral deberá entregar a la entidad correspondiente cualquier tipo de recursos que se le hayan asignado durante su estancia, ya sean materia prima, equipos, respaldos lógicos o cualquier otro tipo de información

17 Políticas de incidentes graves

Políticas:

17.1 Queda prohibido obtener privilegios o el control de cuentas del sistema, sin que se le haya otorgado explícitamente por el administrador.

17.2 Es una falta grave el difundir, copiar, o utilizar información confidencial para otro propósito ajeno al cual está destinada.

17.3 Se prohíbe cualquier tipo de ataque o intento de explotar alguna vulnerabilidad a equipos de cómputo, así mismo infectar intencionalmente cualquier punto de la infraestructura de datos de ITIFE con algún tipo de malware o modificar las configuraciones de algún tipo de equipo de cómputo sin ser autorizado para realizar dicho cambio.

17.4 Es causa de sanción el provocar cualquier tipo de daño intencional a los medios de comunicación de la red.

17.5 Todo incidente detectado debe ser comunicado a la oficina de informática.

17.6 Las faltas a estas políticas serán investigadas por la oficina de informática.

SANCIONES

Las sanciones a que están sujetos todo el personal que labora en ITIFE y que tenga acceso a sistemas informáticos por incumplimiento de sus obligaciones e incurrir en falta a las Políticas señaladas en este documento, son las siguientes:

I. Llamada de atención de manera verbal o escrita.

II. Suspensión de recursos o en su caso equipos de cómputo.

III. Reposición o pago de los bienes extraviados, destruidos o deteriorados.

Adicionalmente de las sanciones que se estipulan en este documento, también están sujetos a las que de manera interna cada oficina o departamento estipulen en sus propios reglamentos.

GLOSARIO

Dirección IP: Secuencia de caracteres empleadas por el protocolo IP (Internet Protocol), para identificar un dispositivo dentro de la red.

Dirección física o dirección MAC: Secuencia de caracteres cuyo fin es identificar a un equipo de otros, por sus siglas en inglés Medium Access Control.

SSID: Nombre que identifica una red de la otra (Service Set IDentifier.).

Incidente: Se considera como un incidente a cualquier falta o incumplimiento a las políticas establecidas en este documento.

IP Homologada: Dirección IP cuyo segmento corresponde a las redes públicas y que son accesibles desde Internet.

IP no homologada o privada: Dirección IP cuyo segmento corresponde a las redes locales y que no son accesibles desde la Internet.

Malware: Código generado con fines maliciosos, entre los que ubicamos: virus, caballos de troya, gusanos, spyware, etc.

Punto de Acceso (Access Point) o PA: Dispositivo de red que permite la conexión de manera inalámbrica a la red.

.**UPS:** Por sus siglas en inglés Uninterruptible Power Supply es un dispositivo de suministro eléctrico que cuenta una batería con la finalidad de proporcionar energía *a un dispositivo en el caso de interrupción o falla del suministro principal.*