REGLAMENTO DE USO DE ACTIVOS DE TI

Capítulo I

Generalidades

Artículo 1. El presente reglamento tiene como **propósito** establecer los términos en los que se establece el uso de los activos de Tecnología de la Información (TI) de la UNIVERSIDAD POPULAR AUTÓNOMA DEL ESTADO DE PUEBLA A.C. en conjunto con su cultura establecida de comportamiento ético y legal, confianza e integridad y de acuerdo con lo dispuesto en la Política de Seguridad de la Información.

Artículo 1bis. El presente reglamento se ajusta a los siguientes documentos normativos:

- Política de Seguridad de la Información
- Política de Uso de Correo Electrónico, Políticas Generales de Comunicación Interna y Lineamientos y procedimientos para el envío masivo de correos electrónicos UPAEP
- Lineamientos y recomendaciones de uso de Recursos de Videoconferencia.

Artículo 2. Se consideran activos de TI cualquier dispositivo informático, infraestructura de red, enlaces, sistemas de comunicación y colaboración, sistemas de videoconferencia, tratamiento de información y almacenamiento, y cualquier otro recurso de hardware o software que basado en tecnologías de la información y comunicaciones se utilicen en la actividad diaria de la Universidad ayudando a cumplir misiones, metas e iniciativas y que deberán ser administrados de manera responsable para asegurar su confidencialidad, integridad y disponibilidad (al final del presente reglamento se incluye un Glosario con términos utilizados en este reglamento).

Artículo 3. El cumplimiento del presente reglamento es obligatorio para toda la comunidad universitaria, el personal contratado por terceros y en general para cualquier usuario que haga uso de algún activo de TI de UPAEP.

Artículo 4. Este reglamento se aplica a los activos de TI administrados por UPAEP, así como los dispositivos personales que se conecten a la infraestructura de red, residan en un servidor de la institución o sean utilizados para el desarrollo de la actividad institucional.

Artículo 5. El marco normativo al que se ajusta el presente reglamento será:

A. ITIL v3 – ISM
B. ISO/IEC 27001:2013: según lo dispuesto en el Anexo 5.1 Orientación de la dirección para la gestión de la seguridad de la información
C. NIST Cybersecurity Framework 1.1: apartado ID.GV-1

Capítulo II

De las obligaciones de los usuarios

Artículo 6. Los usuarios deben ejercer su buen juicio y hacer un uso adecuado y responsable de los activos de TI que UPAEP ponga a su disposición de acuerdo con las políticas y normas establecidas.

Artículo 7. El usuario es responsable de:

I. La seguridad de los datos, cuentas y sistemas bajo su control, debiendo mantener las contraseñas seguras, no compartiendo la información de la cuenta y/o la contraseña.
II. Asegurar la conformación de las contraseñas de acuerdo a la Política de contraseñas de usuario y a la Política de contraseñas y accesos de usuarios privilegiados.
III. Salvaguardar la confidencialidad de los datos de acuerdo a la categoría otorgada.
IV. Garantizar la protección de los activos asignados por UPAEP e informar de inmediato cualquier pérdida o sustracción de estos activos al Centro de Atención de Usuarios UPAEP.
V. Prevenir riesgos, amenazas y vulnerabilidades al acceder al ciberespacio desde la infraestructura de UPAEP.
VI. No afectar el funcionamiento correcto de las operaciones de TI en las actividades de UPAEP.

Artículo 8. El usuario está obligado a permitir que el personal autorizado pueda monitorear, supervisar y auditar el uso de equipos, infraestructura de red, sistemas y almacenamiento y en general los activos de TI. Se prohíbe bloquear activamente los análisis autorizados de auditoría o cualquier mecanismo utilizado para la exploración de los activos de TI.

Artículo 9. La instalación de software no ofrecido por la Plataforma Tecnológica requiere autorización expresa de la misma detallando cuando se realice la solicitud los motivos que lo justifiquen.

Artículo 10. Queda prohibido proporcionar acceso a otra persona, ya sea deliberadamente o por no asegurar su acceso.

Capítulo III

De los activos de TI en general

Artículo 11. Queda prohibido utilizar los recursos de UPAEP para cualquier propósito ilegal o no autorizado, para uso personal o cuando el mismo constituya una actividad delictiva, ilegal o contraria a las normas establecidas en UPAEP. Los activos de TI deben usarse, exclusivamente, para las actividades derivadas de cada uno de los diferentes perfiles de usuario.

Artículo 12. Está prohibido el almacenamiento de información personal en activos institucionales o que viole regulaciones de derechos de autor.

Artículo 13. Los dispositivos que interfieran con otros equipos o usuarios en la red de UPAEP serán desconectados y requisados.

Artículo 14. Se permite el uso de dispositivos personales para el desarrollo de sus actividades institucionales en cuyo caso se deberán de cumplir con todos los lineamientos y normativas de UPAEP.

Artículo 15. En el caso de equipamiento de cómputo, el usuario además de ser responsable del mismo lo será también de todos los accesorios y complementos necesarios para el correcto funcionamiento del equipo, como son cables, fuentes de alimentación, periféricos, etc. velando por su buen estado. En todo momento el usuario debe mantener estos componentes a resguardo para garantizar el funcionamiento.

Artículo 16. Todas las computadoras deben estar protegidas por contraseña con la función de bloqueo automático configurada. Se debe bloquear o cerrar sesión cuando el dispositivo esté desatendido

Artículo 17. Queda terminantemente prohibido interferir con la administración de dispositivos institucionales o el software de seguridad instalado en ellos, como son antivirus, configuraciones de seguridad, etc.

Capítulo IV

De los dispositivos IoT

Artículo 18. Los dispositivos IoT (*Internet of Things*) incorporan elementos que les permiten interactuar con su entorno y ofrecen gran conectividad, lo que a su vez hace que sean sumamente vulnerables pudiendo convertirse fácilmente en punto de acceso a una red. El ciberataque y compromiso de estos dispositivos puede dar lugar a consecuencias graves para la seguridad, como:

- Ser utilizado para realizar ciberataques, por ejemplo, de denegación de servicio distribuida o DDoS
- Ser utilizado como puente o punto de entrada para atacar otros equipos de la misma red, para robar información o comprometer servidores o para realizar otras acciones delictivas
- Alterar su configuración y funcionamiento para que transmitan información alterada.

Artículo 19. El usuario está obligado a informar al Centro de Atención a Usuarios de manera previa a la instalación de dispositivos IoT haciendo constar:

- Justificación de la necesidad de instalación del dispositivo
- Información detallada del dispositivo, como por ejemplo: marca, fabricante, modelo, diagrama de funcionamiento, requerimientos de conexión a la red, número de serie, dirección física (MAC Address) y cualquier otro dato relevante
- Datos del responsable del dispositivo
- Fecha en la que dejará de utilizarse si se conoce

Una vez conectado el dispositivo el responsable del equipo está obligado a:

I. Comunicar a Plataforma tecnológica cualquier incidente detectado en el funcionamiento del dispositivo, desconexión o sustitución del mismo ya sea por avería, mejora o cualquier otra circunstancia.
II. Mantener continuamente actualizado el dispositivo y desconectarlo si por alguna circunstancia o por haber alcanzado el fin de vida útil establecido por el fabricante no pudiera ser actualizado.
III. Sustituir credenciales por defecto, estableciendo contraseñas de acceso y administración robustas. Si el dispositivo ofrece multifactor de autenticación es obligatorio su activación.
IV. Configurar la conexión a la red de UPAEP de acuerdo a lo establecido por Plataforma Tecnológica y utilizar solo los servicios autorizados.
V. Garantizar la seguridad física del dispositivo aplicando las medidas necesarias para evitar el acceso y manipulación no autorizado.

VI. Desconectar el dispositivo y notificar a Plataforma tecnológica cuando la necesidad por la que se conectó haya cesado
VII. Comunicar a Plataforma tecnológica cuando se produzca un cambio en el responsable del dispositivo informando de los datos del nuevo.

Es facultad de la Plataforma Tecnológica auditar aleatoriamente los dispositivos IoT, verificando que se ajusten a lo establecido en el presente reglamento. Si un dispositivo IoT, no cumpliera lo especificado en esta política será bloqueado y retirado de la red institucional.

Capítulo V

De los recursos de Videoconferencia

Artículo 20. Se consideran Recursos de Videoconferencia a cualquier dispositivo, aplicación, infraestructura local o en la nube, sistema de colaboración, y cualquier otro recurso de hardware o software que basado en tecnologías de la información permita la comunicación simultánea bidireccional de audio y vídeo, entre grupos/personas situadas en lugares alejados entre sí.

Artículo 21. El usuario debe utilizar los recursos de videoconferencia que UPAEP pone a su disposición de forma responsable, ajustándose a los lineamientos y recomendaciones de uso establecidos en el documento redactado a tal efecto.

Capítulo VI

Del almacenamiento

Artículo 22. Se considera como almacenamiento cualquier espacio electrónico asignado por UPAEP para alojar contenido necesario para llevar a cabo la actividad institucional propia de cada usuario, ya sea académica o administrativa. Son considerados medios de almacenamiento los siguientes:

- Cualquier plataforma de comunicación o colaboración institucional a la que el usuario tenga acceso
- Equipos de cómputo y periféricos de almacenamiento
- Espacio en dispositivos o sistemas de almacenamiento masivos tanto ubicados en UPAEP como de forma externa, por ejemplo en la nube.

Artículo 23. El usuario está obligado a utilizar el espacio de almacenamiento asignado de forma responsable ajustándose a la cuota que le haya sido asignada y de acuerdo con los siguientes lineamientos:

I. Está prohibido el almacenamiento de material que viole o infrinja derechos de autor o propiedad intelectual
II. Está prohibido el almacenamiento de información de carácter personal
III. El espacio de almacenamiento se dedicará exclusivamente a material necesario para llevar a cabo la actividad desarrollada en UPAEP
IV. La cantidad de espacio ocupado no podrá superar el límite asignado
V. Se podrán llevar a cabo, por parte de la Plataforma Tecnológica, revisiones del contenido almacenado para verificar que se ajusta a lo establecido en la presente Política. En el caso de infringir lo dispuesto en el presente reglamento, el área de Plataforma Tecnológica tiene la facultad de borrar la información que exceda o viole lo establecido.

Capítulo VII

De la infraestructura de la red de comunicaciones

Artículo 24. El usuario es responsable de la seguridad y el uso apropiado de los recursos de red de UPAEP bajo su control. Está estrictamente prohibido utilizar los recursos de UPAEP para lo siguiente:

I. Causar una brecha de seguridad en UPAEP u otros recursos de red, incluidos, entre otros, el acceso a datos, servidores o cuentas para las que no está autorizado; eludir la autenticación de usuario en cualquier dispositivo o rastrear el tráfico de la red.
II. Causar una interrupción del servicio a UPAEP u otros recursos de la red mediante mecanismos de inundaciones de ICMP, ataques de denegación de servicio (distribuido o no) o cualquier otro similar con fines maliciosos.
III. Introducción de *honeypots*, *honeynets* o tecnología similar en la red UPAEP.
IV. Llevar a cabo cualquier actividad que no esté dentro del ámbito académico o administrativo de la Institución.
V. Violar la ley de derechos de autor, que incluye, entre otros, duplicar o transmitir ilegalmente imágenes, música, videos y software con derechos de autor.
VI. Exportar o importar software, información técnica, software de cifrado o tecnología en violación de las leyes de control de exportaciones internacionales o regionales.
VII. Uso de la red de Internet o UPAEP que viole las políticas establecidas en UPAEP o la normativa que sea de aplicación.
VIII. Introducir intencionalmente código malicioso, incluidos, entre otros, virus, gusanos, caballos de Troya, software espía, registradores de pulsaciones de teclas, etc.

IX. Escaneo de puertos o escaneo de seguridad en una red de producción a menos que sea autorizado previamente por Seguridad de la Información.

X. Utilizar mecanismos que eviten el monitoreo, supervisión o protección de las comunicaciones, como proxy o redes privadas virtuales no institucionales, etc.

XI. Cualquier uso del equipamiento de red que no esté contemplado en el perfil del usuario de la Comunidad Universitaria.

XII. Hacer uso de los recursos del Internet de forma no ética e inaceptable de acuerdo a lo dispuesto en el código de ética RFC 1087 del IETF (*Internet Engineering Task Force*) y que incluiría las siguientes conductas:

a. buscar obtener acceso no autorizado a los recursos de Internet,
b. interrumpir el uso previsto de Internet,
c. desperdiciar recursos (personas, capacidad, computadora) a través de tales comportamientos,
d. atentar contra la integridad de la información almacenada en una computadora,
e. comprometer la privacidad de los usuarios.

Capítulo VIII

De las comunicaciones electrónicas

Artículo 25. Queda estrictamente prohibido:

I. Envío de spam por correo electrónico, mensajes de texto, páginas, mensajes instantáneos, correo de voz u otras formas de comunicación electrónica.

II. Realizar envíos de correo electrónico de forma masiva que no se ajusten a la normativa establecida por la Dirección General de Promoción y Comunicación Estratégica.

III. Hacer uso indebido de los medios de comunicación electrónico para fines diferentes al propósito institucional.

IV. Falsificar, tergiversar, ocultar, suprimir o reemplazar la identidad de un usuario en cualquier comunicación electrónica para engañar al destinatario sobre el remitente.

V. Uso de una dirección institucional de correo electrónico o dirección IP de UPAEP para participar en una conducta que viole cualquier tipo de política, norma o ley.

La violación a alguna de las disposiciones anteriomente explicadas que presuntamente constituyan un ilicito podrán ser puestas en conocimiento de las autoridades competentes para los fines legales a los que de lugar.

Artículo 26. Se requerirá autorización expresa de la Dirección General de Promoción y Comunicación Estratégica y siempre de acuerdo con sus políticas, para publicar en nombre de UPAEP en un grupo de noticias, blog, red social, tablón de anuncios o cualquier otra herramienta o plataforma de comunicación.

Capítulo IX

De las sanciones

Artículo 27.- Cualquier violación e incumplimiento a lo previsto en este reglamento será sancionado con:

II. Amonestación escrita

III. Suspensión temporal del servicio, herramienta, acceso o uso del activo de TI, en caso de persistir en la falta o no atender las indicaciones. En este caso se notificará también al superior inmediato en caso de tratarse de un colaborador, al Director Académico en caso de tratarse de un estudiante o al Departamento de Adquisiciones en caso de tratarse de un proveedor.

   En caso de persistir en la falta o no atender las indicaciones:

   a. En el caso de Colaboradores no cumplir con las políticas expresadas en este documento: Remite a quien incumple a lo especificado en el Reglamento de Colaboradores UPAEP Capítulo I artículos 85 a 87.
   b. En el caso de Estudiantes: De acuerdo con lo dispuesto en el artículo 13, Capítulo V del Reglamento General de Estudiantes y Usuarios de Servicios Académicos.
   c. En el caso de Terceros: Lo que se establezca en el Contrato de Prestación de servicios o adquisición y Acuerdos de Confidencialidad que se haya establecido con el mismo.

IV. Reparación del daño causado cuando se amerite.

Artículo 29.- Cuando la gravedad del acto trasciende a la competencia universitaria la institución o quien resulte agraviado podrá acudir ante la autoridad competente para el ejercicio de sus derechos.

Transitorios

Primero.- Se abrogan todas las disposiciones que se opongan al presente**.**

Segundo.- El presente reglamento surtirá efecto a partir de su publicación en las Tablas Oficiales de Avisos de la Universidad.

Tercero.- Las disposiciones contenidas en este ordenamiento son de carácter enunciativo más no limitativo por lo que cualquier situación que afecte los intereses institucionales será resuelta conforme a la normativa universitaria aplicable al caso.

Promulgación

Dado y promulgado en la Ciudad de Puebla, Puebla a los 23 días del mes de marzo del año 2022.

Mtro. José Antonio Llergo Victoria

Secretario General

Mtra. Paola Ochoa Márquez

Directora General de Gestión y Finanzas

Glosario

- Activo de TI: Cualquier equipo, dispositivo, accesorio o entidad de tecnología de la información que tiene valor potencial o real para una organización y que es necesario para el desarrollo de las actividades de la misma.
- Acuerdo de Licencia de Usuario, es un acuerdo de uso del software entre un usuario y un proveedor, estos acuerdos protegen al vendedor del software de las reclamaciones derivadas del comportamiento de software imperfecto.
- Amenaza es cualquier acción que podría dañar un activo. Los sistemas de información enfrentan amenazas tanto naturales como inducidas por el usuario. Las amenazas de origen del usuario a un sistema informático incluyen virus, códigos maliciosos y acceso no autorizado.
- Ataque DOS y DDOS: Ataque de Denegación de Servicio (Denial Of Service) y Ataque Distribuido de Denegación de Servicio (Distributed Denial Of Service). En estos ataque se generan una cantidad masiva de peticiones a un servicio desde una misma máquina o dirección IP (DOS) o desde un gran número de equipos o direcciones IP (DDOS) pudiendo llegar provocar la saturación de ese servicio al superar su capacidad de respuesta lo que conlleva a rechazar peticiones materializando la denegación del servicio.
- Caballos de Troya: Un programa de computadora que lleva dentro de sí mismo un medio para permitir el creador del programa accede al sistema que lo utiliza
- Código malicioso: cualquier software dañino, nocivo o no autorizado diseñado para infiltrarse y dañar un sistema informático.
- Comunidad Universitaria: todas las personas dentro del Sistema UPAEP incluyendo a estudiantes, profesores, colaboradores y proveedores de bienes y servicios.
- Confidencial: información o datos propiedad de UPAEP y que solo los miembros de UPAEP autorizados la pueden ver..
- Datos privados: datos sobre miembros de la comunidad UPAEP que deben mantenerse privados.
- Datos de dominio público: información o datos compartidos como el contenido de sitios WEB y redes sociales de la institución.
- Disponibilidad: los miembros de la comunidad UPAEP autorizados pueden acceder a la información siempre que soliciten la información.
- Escaneo de puertos: mecanismo mediante el cual un dispositivo conectado a una red buscar puertos o servicios abiertos en los equipos o dispositivos
- Gusanos: Un programa de computadora que se replica a sí mismo y es auto-propagador. Los gusanos, a diferencia de los virus, están destinados a generarse en entornos de red.
- Honeypot: Es una herramienta instalada en una red que sirve como señuelo para atraer ataques permitiendo así una detección temprana de actividad maliciosa y desviar la atención de los atacantes de los sistemas importantes. Un honeynet es un tipo especial de honeypot pero implementado en una red completa.

- Inundaciones de ICMP: consiste en saturar una línea de comunicación con un número excesivo de paquetes ICMP (Internet Control Message Protocol, protocolo de mensajes de control de internet)
- IoT: (en inglés Internet of Things) cualquier objeto cotidiano que lleva incorporados sensores, software y otras tecnologías que le permiten captar, recibir y compartir información de forma digital. Por ejemplo pueden ser cámaras de videovigilancia, sensores, electrodomésticos, vehículos, etc.
- ISO/IEC: International Organization for Standardization e International Electrotechnical Commission. Son organismos internacionales de estandarización y normalización, emisores de normas internacionales sobre diferentes aspectos.
- Integridad: sólo los miembros de la comunidad UPAEP autorizados pueden cambiar la información.
- ITIL: (Information Technology Infrastructure Library) es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI)
- NIST: (National Institute of Standards and Technology) es una agencia perteneciente al Departamento de Comercio de los Estados Unidos que ha publicado un marco de seguridad cibernética, que es una guía voluntaria basada en estándares, pautas y prácticas existentes para que las organizaciones administren y reduzcan mejor el riesgo de ciberseguridad.
- Periféricos: Son todos aquellos dispositivos electrónicos conectados a una computadora o un sistema informático que son necesarios para que este realice su actividad. Por ejemplo: monitor, teclado, impresora, etc.
- Programas registradores de pulsaciones de teclas o keylogger: Un keylogger es un software que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado.
- Proxy: dispositivo de red situado entre el equipo de origen y el de destino que permite evitar funciones de filtrado y control de comunicaciones.
- Red privada virtual (VPN): es un sistema cerrado de comunicaciones entre el usuario final y el dispositivo que proporciona el servicio. Es virtual por que no existe una infraestructura física de red si no que utiliza una ya existente.
- RFC 1087: Ética e Internet, en enero de 1989, la Junta de Arquitectura de Internet (IAB) define una actividad como poco ética e si:
    a. Busca tener acceso no autorizado a los recursos de Internet
    b. Interrumpe el uso previsto del Internet
    c. Desperdicia recursos (personas, capacidad, cómputo) a través de tales acciones
    d. Destruye la integridad de la información basada en computadora y/o compromete la privacidad de los usuarios
- Riesgo es la probabilidad de que algo malo le suceda a un activo. Es el nivel de exposición a algún evento que tiene un efecto sobre un activo. En el contexto de seguridad de TI, un activo puede ser una computadora, una base de datos o información. Ejemplos de riesgos incluyen: Perder datos, perder información para el correcto funcionamiento de la institución, no cumplir con las leyes y regulaciones.

- Software espía o spyware: software diseñado para recopilar datos de un ordenador u otro dispositivo y re enviarlos a un tercero sin el conocimiento o consentimiento del usuario.
- Solo uso interno: información o datos compartidos internamente por UPAEP.
- Videoconferencia: tecnología multimedia síncrona que, mediante la compresión digital, en tiempo real, de los flujos de audio, datos y vídeo permite a dos interlocutores o más comunicarse simultáneamente, independientemente de su posición geográfica. Se usa también el término videoconferencia para hacer referencia a la propia llamada mediante la que se comunican los propios interlocutores.
- Virus: Un programa que se replica a sí mismo en los sistemas informáticos incorporándose a otros programas que se comparten entre los sistemas informáticos y cuya finalidad es causar daño.
- Vulnerabilidad es una debilidad que permite que se realice una amenaza o que tenga un efecto sobre una activo. Las vulnerabilidades a menudo pueden dar lugar a responsabilidades legales. Cualquier vulnerabilidad que permita que se realice una amenaza puede dar lugar a acciones legales.
- UPAEP o Sistema UPAEP: Universidad Popular Autónoma del Estado de Puebla A.C que incluye a los niveles de educación media superior (Preparatoria), Licenciatura, Posgrado y a las entidades que se adhieran oficialmente a dicha razón social.