Al margen Escudo del Estado de México y un logotipo que dice: Universidad Intercultural del Estado de México.

El Consejo Directivo, con fundamento el Articulo 11, fracción V, del Decreto del Ejecutivo del Estado por el que se Crea el Organismo Público Descentralizado de Carácter Estatal Denominado Universidad Intercultural del Estado de México expide el siguiente.

MANUAL DE POLÍTICAS Y GUÍA DE SEGURIDAD DE INFORMÁTICA PARA LAS Y LOS USUARIOS DE LA UNIVERSIDAD INTERCULTURAL DEL ESTADO DE MÉXICO

CONTENIDO

4.6. Bases de Datos
4.7. Respaldos de información de Bases de Datos
4.8. Control de acceso a sistemas automatizados de información

5. Política y Guía de Cumplimiento de Seguridad Informática
Política
5.1. Derechos de Propiedad Intelectual
5.2. Revisiones del cumplimiento
5.3. Violaciones de seguridad informática

6. Aprobación
Anexo 1.
Anexo 2.
Restrictivo
Social y Media
Estudiantes

Para los efectos del presente manual, se escribe el presente glosario de términos:

Glosario de Términos

A) **Acceso**: Es el privilegio de una persona para utilizar un objeto o una infraestructura

Acceso Físico: Es la actividad de ingresar a un área.
Acceso Lógico: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque: Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.

B) **Base de datos**: Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

C) **Confidencialidad**: Se refiere a la obligación de los servidores judiciales a no divulgar información a personal no autorizado para su conocimiento.

Contraseña: Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.
Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.
Copyright: Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.

D) **Dirección**: Se refiere a la Dirección de Administración y Finanzas de la Universidad Intercultural del Estado de México.

Disponibilidad: Se refiere a que la información esté disponible en el momento que se necesite

E) **Estándar**: Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

F) **Falta administrativa**: Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor judicial, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.

FTP: Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.

G) **Gusano**: Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

H) **Hardware**: Se refiere a las características técnicas y físicas de las computadoras.

Herramientas de seguridad: Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

I) **Identificador de Usuario**: Nombre de la usuaria o usuario (también referido como UserID) único asignado a un servidor judicial para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.

Impacto: Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad: Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet: Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (world wide web) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión: Es la acción de introducirse o acceder sin autorización a un activo.

M) **Maltrato**: Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la Universidad Intercultural del Estado de México. Se contemplan dentro de éste al descuido y la negligencia.

Malware: Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, spyware, troyanos, rootkits, backdoors, adware y gusanos.
Mecanismos de seguridad o de control: Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir control la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamiento magnéticos: Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)
Módem: Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

N) **"Necesidad de saber" principio**: Es un principio o base de seguridad que declara que las y los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.

Normatividad: Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.

P) **Passport**: Véase Contraseña.

R) **Respaldo**: Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo: Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

S) **Servidor**: Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sitio Web: El sitio web es un lugar virtual en el ambiente de internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software: Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Spyware: Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.

U) **UserID**: Véase Identificador de Usuario.

Usuario: Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).

V) **Virus**: Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.

Vulnerabilidad: Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

Propósito

El presente documento tiene como finalidad dar a conocer las políticas y la Guía de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Universidad Intercultural del Estado de México.

Introducción

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

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Universidad Intercultural del Estado de México en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para las y los usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal
- Seguridad Física y Ambiental
- Administración de Operaciones de Cómputo
- Controles de Acceso Lógico
- Cumplimiento

Estas Políticas en seguridad informática se encuentran alineadas con el Estándar ISO 27002.

Objetivo

Establecer y difundir las Políticas y Guía de Seguridad Informática a todo el personal de la Universidad Intercultural del Estado de México, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

Alcance

El documento define las Políticas y Guía de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de la Universidad Intercultural del Estado de México.

Justificación

El Departamento de Informática de la Universidad Intercultural del Estado de México está facultado para definir Políticas y la Guía en materia informática.

Sanciones por Incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

Las Políticas y Guía de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información de la Universidad Intercultural del Estado de México.

1. Políticas y Guía de Seguridad del Personal

Política

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la Universidad Intercultural del Estado de México, así como el estricto apego al Manual de Políticas y Guía de Seguridad Informática para usuarios.

1.1. Obligaciones De los Usuarios. Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Guía de Seguridad Informática para Usuarios del presente manual.

1.2. Acuerdos de uso y confidencialidad. Todos los usuarios de bienes y servicios informáticos de la Universidad Intercultural del Estado de México, deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de esta Universidad, así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Guía de Seguridad Informática para las y los Usuarios

1.3. Entrenamiento en Seguridad Informática. Todo empleado del Universidad Intercultural del Estado de México de nuevo ingreso deberá: Leer el Manual de Políticas y Guía de Seguridad Informática para las y los Usuarios de la Universidad Intercultural del Estado de México, el cual se encuentra disponible en el portal de internet UIEM, donde se dan a conocer las obligaciones para las y los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

1.4. Medidas disciplinarias Cuando el Departamento de Informática identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Comité de Honor y Justicia de la Universidad Intercultural del Estado de México, para los efectos de su competencia y atribuciones.

2. Política y Guía de Seguridad Física

Política

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Universidad Intercultural del Estado de México, sólo a personas autorizadas para la salvaguarda de los

equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes Centros de Cómputo de la Universidad Intercultural del Estado de México.

2.1. Resguardo y protección de la información

2.1.1. La y el usuario deberá reportar de forma inmediata al Departamento de Informática, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2. La y el usuario tiene la obligación de proteger los CD-ROM, DVD, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su resguardo y administración, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Universidad Intercultural del Estado de México que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2. Controles de acceso físico. Cualquier persona que tenga acceso a las instalaciones de la Universidad Intercultural del Estado de México, deberá registrar en el la Bitácora de Acceso, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Universidad Intercultural del Estado de México, el cual podrán retirar el mismo día, sin necesidad de trámite alguno.

En caso de que el equipo que no es propiedad de la Universidad Intercultural del Estado de México, permanezca dentro de la institución más de un día hábil, es necesario que el responsable del órgano de la Universidad Intercultural del Estado de México en el que trabaja el dueño del equipo, elabore y firme oficio de autorización de salida.

2.3. Seguridad en áreas de trabajo. Los Sites de la Universidad Intercultural del Estado de México son áreas restringidas, por lo que sólo el personal autorizado por el Departamento de Informática puede acceder a ellos.

2.4. Protección y ubicación de los equipos

2.4.1. La o el usuario no debe mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Departamento de Informática, debiéndose solicitar a la misma en caso de requerir este servicio.

2.4.2. El Departamento de Recursos Materiales y Servicios Generales será el encargado de generar el resguardo generados por el SICOPA; en caso de no ser bienes que se encuentren bajo el resguardo del Departamento de Informática y que no cuenten con el resguardo del SICOPA, se debe generar un resguardo interno (ver Anexo 1); así mismo, recabar la firma del usuario como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por ésta área.

2.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario de la Universidad Intercultural del Estado de México.

2.4.4. Será responsabilidad de la y el usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.4.5. Es responsabilidad de la y el usuario almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.6. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.

2.4.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.4.9. Las y los usuarios deben asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.4.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al Departamento de Informática a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.4.11. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.5. Mantenimiento de equipo

2.5.1 Únicamente el personal autorizado de Informática podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2 Las y los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de Informática.

2.6. Pérdida o transferencia de equipo

2.6.1 La y 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.

2.6.2 El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3 La y el usuario deberá dar aviso de inmediato a Informática de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales

2.7.1 El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.7.2 La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

2.7.3 La y el usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.8. Daño del equipo. El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha descompostura, siendo el Departamento de Informática el encargado de evaluar el daño y emitir dictamen de reparación del mismo.

3. Política de Seguridad y Operación de Equipo de Computo

Política

Las y los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Universidad Intercultural del Estado de México. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Universidad Intercultural del Estado de México o hacia redes externas como internet.

Las y los usuarios de la Universidad Intercultural del Estado de México que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. La o el usuario puede acudir al Departamento Informática, o al representante de ésta en su zona, para solicitar asesoría.

3.1. Uso de medios de almacenamiento

3.1.1 Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del jefe inmediato del usuario y del titular del área dueña de la información. Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con sello y firma del titular de área.

3.1.2 Las y los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de Informática o al representante de ésta en su zona, para que dichos asesores determinen el medio en que se realizará el respaldo.

3.1.3 En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito al Titular del Departamento de Informática, y deberá contar con la firma del titular del área de adscripción del solicitante.

3.1.4 Los trabajadores de la Universidad Intercultural del Estado de México deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita la Unidad de Acceso a la Información Pública de la Universidad Intercultural del Estado de México, en términos de Ley de Acceso a la Información pública del Estado de México, Acuerdo General que establece el órgano, y demás criterios y procedimientos establecidos en esta materia.

3.1.5 Las actividades que realicen los usuarios de la Universidad Intercultural del Estado de México en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

3.2. Instalación de Software

3.2.1 Las y los usuarios que requieran la instalación de software que no sea propiedad de la Universidad Intercultural del Estado de México, deberán justificar su uso y solicitar su autorización al Departamento de Informática, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software acredite la licencia y/o clave de activación para su uso,

Si el dueño del software no presenta la licencia y/o clave de activación del software, el personal asignado por la Dirección procederá de manera inmediata a desinstalar dicho software.

3.2.2 Se considera una falta grave el que las y los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Universidad Intercultural del Estado de México, que no esté autorizado por el Departamento de Informática.

3.3. Identificación del incidente

3.3.1 La o el usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Departamento de Informática o al representante de ésta en su zona, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, la o el usuario informático deberá notificar al titular de su adscripción.

3.3.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Universidad Intercultural del Estado de México, debe ser reportado al Departamento de Informática.

3.4. Administración de la configuración. Las y los usuarios de las áreas de la Universidad Intercultural del Estado de México no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Universidad Intercultural del Estado de México, sin la autorización por escrito del Departamento de Informática.

3.5. Seguridad de la red. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Departamento de Informática en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la Universidad Intercultural del Estado de México, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

3.6. Uso del correo electrónico

3.6.1 Las y los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Universidad Intercultural del Estado de México, a menos que cuente con la autorización del titular del área de adscripción.

3.6.2 Las y los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Universidad Intercultural del Estado de México (si es propiedad de la Universidad Intercultural del Estado de México del Estado es información pública). Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3 Las y los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el Departamento de Informática.

3.6.4 La Universidad Intercultural del Estado de México, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la Universidad Intercultural del Estado de México o realizado acciones no autorizadas. Como la información del correo electrónico institucional de la Universidad Intercultural del Estado de México es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.6.5 La y el usuario debe de utilizar el correo electrónico y la cuenta de office 365 de la UIEM, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.6 La asignación de una cuenta de correo electrónico, deberá solicitarse por escrito al Departamento de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda.

3.6.7 Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso

3.7.1 Para prevenir infecciones por virus informáticos, los usuarios de la Universidad Intercultural del Estado de México, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Dirección.

3.7.2 Las y los usuarios de la Universidad Intercultural del Estado de México, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, CD´s, DVD's, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por Informática.

3.7.3 La y el usuario debe verificar mediante el software de antivirus autorizado por Informática que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

3.7.4 Ninguna usuaria o usuario de la Universidad Intercultural del Estado de México debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la Universidad Intercultural del Estado de México. El incumplimiento de este estándar será considerado una falta grave.

3.7.5 Ninguna usuaria o usuario ni empleada como empleado, de la Universidad Intercultural del Estado de México o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Departamento de Informática.

3.7.6 Cualquier usuaria o usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Departamento de Informática para la detección y erradicación del virus.

3.7.7 Cada usuaria o usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica a la Dirección las actualizaciones del software de antivirus.

Las y los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas en programas tales como:

- Antivirus
- Correo electrónico
- Paquetería Office
- Navegadores
- Otros programas

Debido a que algunos virus son extremadamente complejos, ninguna usuaria o usuario de la Universidad Intercultural del Estado de México debe intentar erradicarlos de las computadoras, lo indicado es llamar al personal de la Dirección para que sean ellos quienes lo solucionen.

3.8. Permisos de uso de Internet

3.8.1 El acceso a internet provisto a los usuarios de la Universidad Intercultural del Estado de México es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Autoridad de la Universidad Intercultural del Estado de México.

3.8.2 La asignación del servicio de internet, deberá solicitarse por escrito a la Dirección de Administración y Finanzas, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

3.8.3 Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Universidad Intercultural del Estado de México.

3.8.4 Los y los usuarios con acceso a Internet de la Universidad Intercultural del Estado de México tienen que reportar todos los incidentes de seguridad informática al Departamento de Informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.5 El acceso y uso de WiFi en la Universidad Intercultural del Estado de México tiene que ser previamente autorizado por la Dirección de Administración y Finanzas.

3.8.6 Los y 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 Informática.
- La utilización de internet es para el desempeño de su función y puesto en Universidad Intercultural del Estado de México y no para propósitos personales.

3.8.7 Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

- Directores: Sin restricciones: Los y los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.
- Administrativos: Internet restringido y mensajería instantánea: Las y los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación denominada *"Restrictivo"* ver anexo 2.
- Docentes: Internet restringido y sin mensajería instantánea: Las y los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación denominada *"Social y Media"* ver anexo 2.
- Alumnos: Internet restringido y sin mensajería instantánea: La usuaria o usuario solo podrá navegar en sitios de interés educativo aplicándose las políticas de seguridad y navegación denominada *"Estudiantes"* ver anexo 2.

4. Política y Guía de Control de Acceso Lógico

Política

Cada usuaria o usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica de la Universidad Intercultural del Estado de México, por lo cual deberá mantenerlo de forma confidencial.

La Rectoría de la Universidad Intercultural del Estado de México, es la única que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la Universidad Intercultural del Estado de México, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

4.1. Controles de acceso lógico

4.1.1 El acceso a la infraestructura tecnológica de la Universidad Intercultural del Estado de México para personal externo debe ser autorizado al menos por un titular de área de la Universidad Intercultural del Estado de México, quien deberá notificarlo por oficio al Departamento de Informática, quien lo habilitará.

4.1.2 Está prohibido que las y los usuarios utilicen la infraestructura tecnológica de la Universidad Intercultural del Estado de México del Estado para obtener acceso no autorizado a la información u otros sistemas de información de la Universidad Intercultural del Estado de México.

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

4.1.4 Todas las usuarias y usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Departamento de Informática antes de poder usar la infraestructura tecnológica de la Universidad Intercultural del Estado de México.

4.1.5 Todas las usuarias y usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Universidad Intercultural del Estado de México, a menos que se tenga autorización de la Dirección de Administración y Finanzas.

4.1.6 Cada usuaria y usuario que accede a la infraestructura tecnológica de la Universidad Intercultural del Estado de México debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

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

4.1.8 Las y los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de privilegios. Cualquier cambio en los roles y responsabilidades de las y los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la Universidad Intercultural del Estado de México, deberán ser notificados por escrito o vía correo electrónico a la Unidad de Informática con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido. Las y los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la Unidad de Informática, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.4. Administración y uso de contraseñas

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

4.4.2 Cuando una usuaria o usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la Unidad de Informática, indicando si es de acceso a la red o a módulos de sistemas desarrollados por la Dirección, para que se le proporcione una nueva contraseña.

4.4.3 La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el DI como empleado de la Universidad Intercultural del Estado de México del Estado.

4.4.4 Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.4.5 Todas las usuarias y usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos.
- Deben estar compuestos de al menos ocho (8) caracteres. Estos caracteres deben ser alfanuméricos, es decir números y letras.
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.6 La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

4.4.7 Toda usuaria y usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.
4.4.8 Las usuarias y usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.
4.4.9 Los cambios o desbloqueo de contraseñas solicitados por la o el usuario a la Dirección serán solicitados mediante oficio sellado y firmado por el jefe inmediato del usuario que lo requiere.

4.5. Control de accesos remotos
4.5.1 Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del Departamento de Informática.
4.5.2 La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Unidad de Informática.

4.6. Bases de Datos
4.6.1 El administrador de Base de Datos, no debe eliminar ninguna información del sistema automatizado de información si no existe la autorización previa de Rectoría y el Departamento responsable del sistema automatizado de información.
4.6.2 El administrador de la Base de Datos es el encargado de asignar las cuentas de los usuarios.
4.6.3 Las contraseñas serán asignadas por el administrador de la Base de Datos en el momento en que la o el usuario desee activar su cuenta, mediante solicitud previa enviada al Jefe Inmediato del Departamento de responsable del sistema automatizado.
4.6.4 En caso de olvido de contraseña de un usuario, será necesario seguir el procedimiento establecido por el departamento responsable.

4.7. Respaldos de información de Bases de Datos
4.7.1 El administrador de las Bases de Datos del sistema automatizado debe realizar respaldos periódicamente en forma automática y manual, según los procedimientos generados para tal efecto, llevar un registro histórico de los mismos, indicando como mínimo: fecha, hora, nombre del responsable, descripción del contenido respaldado, medio de respaldo y lugar de alojamiento del mismo, así como un instructivo para su restauración. En caso de requerir restaurar información, es responsabilidad del usuario efectuar la misma llevando un registro en el que se indique como mínimo: fecha, hora, nombre de quien restaura y motivo de la restauración.
4.7.2 Los demás respaldos de las Bases de Datos (una copia completa) deben ser almacenados en un lugar seguro bajo los estándares de calidad para almacenamiento de medios magnéticos, que garanticen su preservación.

4.8. Control de acceso a sistemas automatizados de información
4.8.1 Cumplirlas políticas sobre contraseñas establecida en el punto 4.4
4.8.2 Almacenar las contraseñas cifrándolas una sola vez para evitar que sean fácilmente descubiertas. Si las contraseñas son distribuidas de forma electrónica a lo largo de las redes, las mismas deben ser cifradas.
4.8.3 Concientizar a las y los usuarios para que cambien sus contraseñas, se debe solicitar que lo hagan inmediatamente después de recibir su contraseña inicial o cuando se emita una nueva contraseña, y de ahí en adelante al menos cada 3 meses.
4.8.4 Debe tomarse en consideración un cambio más frecuente de contraseña, en el caso de aplicaciones críticas tales como los sistemas de pago o nómina, control escolar y el acceso para resolución de problemas a los sistemas automatizados de información. Si en circunstancias excepcionales se autorizan contraseñas compartidas, éstas deben ser cambiadas con prontitud tras su emisión inicial, de igual manera cuando alguno de los usuarios ya no cuente con más autorización para su uso.
4.8.5 Evitar que las y los usuarios seleccionen nuevamente contraseñas que hayan utilizado recientemente para garantizar un grado razonable de cambio regular.
4.8.6 Desplegar un aviso que advierta que sólo las y los usuarios autorizados pueden acceder al sistema y que cualquier acceso no autorizado podría ser considerado como un acto que genere motivo de responsabilidad jurídica.
4.8.7 Evitar desplegar las contraseñas o cualquier otra información que pudiera servir de ayuda para acceder, sin autorización a terminales de computadoras o impresoras.
4**.8.8** Las contraseñas no deben ser registradas en pistas o registros de auditoria.

4.8.9 Suspender los derechos de acceso del usuario:

- Tras tres intentos fallidos consecutivos de inicio de sesión.

- se logra un inicio de sesión en el tiempo máximo establecido.

4.8.10. Suspender los derechos de acceso del usuario que no hayan sido utilizados durante un periodo de 90 días consecutivos. Posteriormente, las cuentas de usuario suspendido deben ser borradas.
4.8.11. Concluir la sesión de las terminales si las mismas permanecen inactivas por más tiempo del estipulado como tiempo máximo. Cuando esto no sea posible, implementar protectores de pantalla protegidos con contraseña.

5. Política y Guía de Cumplimiento de Seguridad Informática

Política
De acuerdo al Reglamento Interno de la Universidad Intercultural del Estado de México: "El Departamento de Informática, es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico al interior de la Universidad Intercultural del Estado de México".

5.1. Derechos de Propiedad Intelectual

5.1.1 Está prohibido por las leyes de derechos de autor y por la Universidad Intercultural del Estado de México, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por la Universidad Intercultural del Estado de México.
5.1.2 Los sistemas desarrollados por personal, interno o externo, que sea parte del Departamento de Informática, o sea coordinado por ésta, son propiedad intelectual de la Universidad Intercultural del Estado de México.

5.2. Revisiones del cumplimiento

5.2.1 El Departamento de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y Guía de Seguridad Informática para usuarios.
5.2.2 El Departamento de Informática podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática

5.3.1 Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Departamento de Informática.
5.3.2 Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Departamento de Informática, con excepción de los Órganos Fiscalizadores.
5.3.3 Ningún usuario de la Universidad Intercultural del Estado de México del Estado debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección.
5.3.4 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para auto replicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la Universidad Intercultural del Estado de México del Estado.

6. Aprobación

TRANSITORIOS

Primero. Publíquese el presente Lineamiento en el Periódico Oficial "Gaceta del Gobierno".

Segundo. El presente Lineamiento entrará en vigor al día hábil siguiente de su publicación en el Periódico Oficial "Gaceta del Gobierno".

El presente Lineamiento fue aprobado por acuerdo del Consejo Directivo en Sesión Ordinaria 103, celebrada del día 06 del mes de julio de dos mil veintiuno.- **DRA. XÓCHITL GUADARRAMA ROMERO, RECTORA Y SECRETARIA DEL CONSEJO DIRECTIVO DE LA UNIVERSIDAD INTERCULTURAL DEL ESTADO DE MÉXICO.- RÚBRICA.**

Anexo 1.

GOBIERNO DEL ESTADO DE MÉXICO

UNIVERSIDAD INTERCULTURAL ESTADO DE MÉXICO

FECHA:	
SALIDA:	
ENTRADA:	

SOLICITUD DE SALIDA DE BIENES		
UNIDAD ADMINISTRATIVA:	DESTINO:	
MOTIVO DE SALIDA		
No. INVENTARIO No. DE SERIE	CARÁCTERÍSTICA DEL BIEN O MATERIAL	CANTIDAD
AUTORIZA	**Vo. Bo.**	**REVISÓ**
Nombre y Firma del Jefe del Departamento **RECURSOS MATERIALES Y SERVICIOS GENERALES**	Nombre y Firma del Responsable **Cargo o Área**	Nombre y firma del Vigilante **VIGILANCIA**

RESPONSIVA: Acepto que he verificado el funcionamiento correcto de los bienes en la presenta solicitud y que en este momento recibo a mi entera satisfacción, obligándome a utilizar dichos bienes exclusivamente en el desempeño de las funciones que me han sido encomendadas y salvaguardar su integridad física. En caso de daño o pérdida de los mismos, me comprometo a dar aviso inmediato al titular del Área Administrativa y a las autoridades competentes que correspondan, cumplir puntual y oportunamente las instrucciones que al respecto me sean dadas y sufragar de mi peculio sin dilación. El costo de las reparaciones en Centros de Servicio Autorizado o reposición de los bienes por otros de idéntica o mayores características. Quedo exceptuado del pago o reposición, siempre y cuando demuestre fehacientemente la existencia de alguna excluyente de responsabilidad a mi favor.

ACEPTO

NOMBRE Y FIRMA

Anexo 2.

Perfiles de firewall

Restrictivo

1. Protección infantil:
   a. Alcohol y tabaco (bloqueado)
   b. Actividades criminales (bloqueado)
   c. Juegos (bloqueado)
   d. Odio e intolerancia (bloqueado)
   e. Drogas ilegales (bloqueado)
   f. Desnudos (bloqueado)
   g. Pornografía y sexualidad explicita (bloqueado)
   h. Violencia (bloqueado)
   i. Armas (bloqueado)
   j. Trampas escolares (bloqueado)
   k. Educación sexual (desbloqueado)
   l. Tasteless (bloqueado)
   m. Imágenes de abuso infantil (bloqueado)

2. Ocio:
   a. Entretenimiento(bloqueado)
   b. Juegos(bloqueado)
   c. Deportes(bloqueado)
   d. Viajes(desbloqueado)
   e. Ocio y recreación(desbloqueado)
   f. Moda y belleza(bloqueado)

3. Negocios:
   a. Negocios(desbloqueado)
   b. Buscador de empleos(desbloqueado)
   c. Web basada en correo(desbloqueado)

4. Chat:
   a. Chat(desbloqueado)
   b. Mensajería instantánea(desbloqueado)

5. Computación:
   a. Anonimizadores(bloqueado)
   b. Grupos de foro(desbloqueado)
   c. Computadoras y tecnologías(desbloqueado)
   d. Sitios de descargas(bloqueado)
   e. Streaming y descargas(bloqueado)
   f. Suplantación y fraude(bloqueado)

g. Portales de búsqueda(desbloqueado)
h. Redes sociales(bloqueado)
i. Sitios de spam(bloqueado)
j. Malware(bloqueado)
k. Botnets(bloqueado)
l. Hackeo(bloqueado)
m. Software ilegal(bloqueado)
n. Información de seguridad(desbloqueado)
o. Redes per to per(bloqueado)

6. Otros:
a. Anuncios y ventanas emergentes(bloqueado)
b. Arte(desbloqueado)
c. Transporte(desbloqueado)
d. Compromised(desbloqueado)
e. Citas personales(desbloqueado)
f. Educación(desbloqueado)
g. Finanzas(desbloqueado)
h. Gobierno(desbloqueado)
i. Salud y medicina(desbloqueado)
j. Noticias(bloqueado)
k. Asociaciones sin fines de lucro y organizaciones internacionales (desbloqueado)
l. Sitios personales(desbloqueado)
m. Política(desbloqueado)
n. Bienes raíces(bloqueado)
o. Religión(desbloqueado)
p. Restaurantes(desbloqueado)
q. Compras(desbloqueado)
r. Traductores(desbloqueado)
s. General(desbloqueado)
t. Culto(desbloqueado)
u. Tarjetas de felicitación(bloqueado)
v. Intercambio de imágenes(desbloqueado)
w. Error de redes(desbloqueado)
x. Parked domains(desbloqueado)
y. Direcciones ip privadas(desbloqueado)
z. Sitios sin categoría(desbloqueado)

Social y Media

1. Protección infantil:
a. Alcohol y tabaco (bloqueado)
b. Actividades criminales (bloqueado)
c. Juegos (bloqueado)
d. Odio e intolerancia (bloqueado)
e. Drogas ilegales (bloqueado)
f. Desnudos (bloqueado)
g. Pornografía y sexualidad explicita (bloqueado)
h. Violencia (bloqueado)
i. Armas (bloqueado)
j. Trampas escolares (bloqueado)
k. Educación sexual (desbloqueado)
l. Tasteless (bloqueado)
m. Imágenes de abuso infantil (bloqueado)
2. Ocio:
a. Entretenimiento(bloqueado)
b. Juegos(bloqueado)
c. Deportes(bloqueado)
d. Viajes(desbloqueado)
e. Ocio y recreación(desbloqueado)
f. Moda y belleza(bloqueado)
3. Negocios:
a. Negocios(desbloqueado)
b. Buscador de empleos(desbloqueado)
c. Web basada en correo(desbloqueado)
4. Chat:
a. Chat(bloqueado)
b. Mensajería instantánea(bloqueado)
5. Computación:
a. Anonimizadores(bloqueado)
b. Grupos de foro(desbloqueado)
c. Computadoras y tecnologías(desbloqueado)
d. Sitios de descargas(bloqueado)
e. Streaming y descargas(bloqueado)
f. Suplantación y fraude(bloqueado)
g. Portales de búsqueda(desbloqueado)
h. Redes sociales(bloqueado)
i. Sitios de spam(bloqueado)
j. Malware(bloqueado)
k. Botnets(bloqueado)
l. Hackeo(bloqueado)
m. Software ilegal(bloqueado)
n. Información de seguridad(desbloqueado)
o. Redes per to per(bloqueado)
6. Otros:
a. Anuncios y ventanas emergentes(bloqueado)
b. Arte(desbloqueado)
c. Transporte(desbloqueado)
d. Compromised(bloqueado)
e. Citas personales(desbloqueado)
f. Educación(desbloqueado)
g. Finanzas(desbloqueado)
h. Gobierno(desbloqueado)
i. Salud y medicina(desbloqueado)

j. Noticias(bloqueado)
k. Asociaciones sin fines de lucro y organizaciones internacionales(desbloqueado)
l. Sitios personales(desbloqueado)
m. Política(desbloqueado)
n. Bienes raíces(bloqueado)
o. Religión(desbloqueado)
p. Restaurantes(desbloqueado)
q. Compras(desbloqueado)
r. Traductores(desbloqueado)
s. General(desbloqueado)

Estudiantes

1. Protección infantil:
   a. Alcohol y tabaco (bloqueado)
   b. Actividades criminales (bloqueado)
   c. Juegos (bloqueado)
   d. Odio e intolerancia (bloqueado)
   e. Drogas ilegales (bloqueado)
   f. Desnudos (bloqueado)
   g. Pornografía y sexualidad explicita (bloqueado)
   h. Violencia (bloqueado)
   i. Armas (bloqueado)
   j. Trampas escolares (bloqueado)
   k. Educación sexual (desbloqueado)
   l. Tasteless (bloqueado)
   m. Imágenes de abuso infantil (bloqueado)

2. Ocio:
   a. Entretenimiento(bloqueado)
   b. Juegos(bloqueado)
   c. Deportes(bloqueado)
   d. Viajes(bloqueado)
   e. Ocio y recreación(bloqueado)
   f. Moda y belleza(bloqueado)

3. Negocios:
   a. Negocios(desbloqueado)
   b. Buscador de empleos(bloqueado)
   c. Web basada en correo(desbloqueado)
4. Chat:
   a. Chat(bloqueado)
   b. Mensajería instantánea(bloqueado)

5. Computación:
   a. Anonimizadores (bloqueado)
   b. Grupos de foro(desbloqueado)
   c. Computadoras y tecnologías(desbloqueado)
   d. Sitios de descargas(bloqueado)
   e. Streaming y descargas(bloqueado)
   t. Culto (bloqueado)
   u. Tarjetas de felicitación (bloqueado)
   v. Intercambio de imágenes (bloqueado)
   w. Error de redes (desbloqueado)
   x. Parked domains (desbloqueado)
   y. Direcciones ip privadas (desbloqueado)
   z. Sitios sin categoría (desbloqueado)

   f. Suplantación y fraude(bloqueado)
   g. Portales de búsqueda(desbloqueado)
   h. Redes sociales(bloqueado)
   i. Sitios de spam(bloqueado)
   j. Malware(bloqueado)
   k. Botnets (bloqueado)
   l. Hackeo(bloqueado)
   m. Software ilegal(bloqueado)
   n. Información de seguridad(bloqueado)
   o. Redes per to per (bloqueado)

6. Otros:
   a. Anuncios y ventanas emergentes(bloqueado)
   b. Arte(desbloqueado)
   c. Transporte(desbloqueado)
   d. Compromised (bloqueado)
   e. Citas personales(bloqueado)
   f. Educación(desbloqueado)
   g. Finanzas(desbloqueado)
   h. Gobierno(desbloqueado)
   i. Salud y medicina(desbloqueado)
   j. Noticias(bloqueado)
   k. Asociaciones sin fines de lucro y organizaciones internacionales(bloqueado)
   l. Sitios personales(bloqueado)
   m. Política(bloqueado)
   n. Bienes raíces(bloqueado)
   o. Religión(bloqueado)
   p. Restaurantes(bloqueado)
   q. Compras(desbloqueado)
   r. Traductores(bloqueado)
   s. General(bloqueado)
   t. Culto(bloqueado)
   u. Tarjetas de felicitación(bloqueado)
   v. Intercambio de imágenes(bloqueado)
   w. Error de redes(bloqueado)
   x. Parked domains (bloqueado)
   y. Direcciones ip privadas(bloqueado)
   z. Sitios sin categoría(desbloqueado)