Normativa acceso Internet y navegación segura

Índice

CONTENIDO

1. OBJETIVO

El objetivo de la presente normativa es regular el acceso a Internet por parte de las personas usuarias de los Sistemas de Información de la Universidad del País Vasco/Euskal Herriko Unibertsitatea, en adelante UPV/EHU, desde sus sedes o a través de ellas, posibilitando unas reglas de uso que deberán ser conocidas y observadas por todos.

Con carácter general, las personas usuarias de la UPV/EHU dispondrán de acceso a Internet como herramienta de productividad y conocimiento en el curso normal de sus funciones en actividades académicas, docentes y de investigación y procesos administrativos y de gestión.

Dos son los principios generales que rigen esta normativa:

- Establecer las normas debidas e indebidas para el uso y manejo de Internet a través de la red de la UPV/EHU, y vigilar su cumplimiento.

- Respetar y proteger de una manera responsable y legal los derechos de las personas usuarias en la comunidad universitaria y en Internet.

Este documento se considera de uso interno de la UPV/EHU y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad.

2. ÁMBITO DE APLICACIÓN

Esta Norma es de aplicación a todo el ámbito de actuación de la UPV/EHU, y sus contenidos traen causa de las directrices de carácter más general definidas en **la Política de Seguridad de la Información de la UPV/EHU**.

La presente Norma será de obligado cumplimiento para todas las personas usuarias que de manera permanente o eventual utilicen los servicios de la UPV/EHU, incluyendo el personal de organizaciones externas cuando sean personas usuarias o posean acceso a los Sistemas de Información de la UPV/EHU.

Todas las personas usuarias dispondrán de acceso a Internet:

- A través de los puestos de trabajo, de los ordenadores de la UPV/EHU que se disponen a tal efecto, respetando siempre las particularidades de cada centro, aula informática o red de acceso.
- Con sus dispositivos personales a través de las redes de uso general o de invitados que se disponen para ello.

La presente Normativa ha sido aprobada por el Comité de Seguridad TIC de la UPV/EHU, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la UPV/EHU pone a disposición de las personas usuarias para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

3. NORMATIVA

3.1 NORMAS GENERALES

El acceso a Internet es un activo de la UPV/EHU suministrado a las personas usuarias como apoyo en la realización de sus funciones en actividades académicas, docentes y de investigación, y en procesos administrativos y de gestión. El uso personal ocasional o eventual de este recurso está permitido, en tanto no interfiera con la productividad propia o ajena y no cause conflictos con la actividad de la UPV/EHU. Toda información transmitida por este medio será tratada como información relacionada con la UPV/EHU y debe estar alineada a las normas enumeradas más abajo.

Para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso.

Tales medidas son:

- Internet debe usarse de manera responsable y para fines profesionales o relacionados con la docencia, investigación y gestión.

- No Acceder a sitios Web que no cumplan con el código de ética de la UPV/EHU, ofensivo o ilegal.

- No descargar desde Internet cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad sin la correspondiente autorización o licencia de derecho usando enlaces directos o programas de tipo “peer-to-peer” (P2P) .

- No publicar cualquier tipo de información perteneciente a la UPV/EHU o en nombre de ésta en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información o de los derechos de uso.

- Se prohíbe el acceso o intento **no autorizado** sobre equipos, servicios, aplicaciones, datos o infraestructuras de la UPV/EHU o ajenos a ella.

- Queda totalmente prohibido la destrucción o modificación premeditada de la información de otras personas usuarias, así como la violación de la privacidad e intimidad de otras personas usuarias.

- **Asegurar la autenticidad de la página visitada**. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Cuando la página web se encuentre autenticada mediante certificado digital (protocolo HTTPS), la persona usuaria verificará su autenticidad.

- **Cerrar las sesiones al terminar la conexión**. Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información, ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otras personas tengan acceso a las cuentas y a la información utilizada durante la sesión no cerrada correctamente. La mayoría de los sitios web disponen de una opción de "desconexión", "logout" o similar que conviene utilizar.

- **Utilizar herramientas contra código dañino**. El volumen de código dañino que circula por Internet es muy elevado y presenta multitud de aspectos diferentes. El uso de un antivirus permanentemente actualizado es la primera protección contra este tipo de ataques. Además de ello, es necesario tener configurado adecuadamente el firewall o cortafuegos, software específico contra programas espía (spyware), etc.

- **Mantener actualizado el sistema operativo, el navegador y las herramientas de seguridad** . Es imprescindible tener actualizado el sistema operativo, así como las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.), con los últimos parches de seguridad emitidos por el fabricante. Puesto que el código dañino se genera incesantemente, es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar al CAU sobre cualquier problema que se detecte en este proceso de actualización.

- **Utilizar los niveles de seguridad del navegador**. Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "medio-alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.

- **Eliminar la información privada**. Los navegadores Web almacenan información privada durante su utilización, tal como el historial de

navegación, cookies aceptadas, contraseñas, etc.; información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.

- **No visitar páginas no fiables o sospechosas**. Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas susceptibles de contener código malicioso.

- **No descargar código o programas no confiables**. Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales.

- **No instalar complementos desconocidos**. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador de la persona usuaria un complemento (plug-in, add-on, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.

- Se deberá informar inmediatamente al Centro de Atención a Usuarios (CAU) de la UPV/EHU sobre cualquier ocurrencia inusual que suceda en el uso de Internet.

3.3 MEDIDAS DE SEGURIDAD

La transmisión de información por la red no siempre es segura. Los niveles de seguridad dependerán del sistema informático que se esté utilizando, que este esté actualizado y que se usen medidas adicionales de seguridad, así como antivirus. Se recuerda que la pérdida de información es responsabilidad de las personas usuarias.

Desde la UPV/EHU se informa sobre los métodos más habituales para evitar pérdidas de información, los accesos no autorizados, etc. En consecuencia:

- Queda terminantemente prohibido compartir con otras personas usuarias las contraseñas y cuentas de correo o acceso.

- Se deben utilizar contraseñas robustas según lo dispuesto en la normativa de creación y uso de contraseñas de la UPV/EHU.

Para proteger a los usuarios finales de la UPV/EHU, así como los servicios expuestos por esta, y garantizar el correcto funcionamiento del acceso a Internet, así como el cumplimiento de esta normativa, la UPV/EHU tomará las medidas técnicas necesarias y disponibles para intentar asegurar la integridad, disponibilidad y confidencialidad de las comunicaciones. Entre otras, existen elementos de gestión, control y monitorización permanente del tráfico entre la red de la UPV/EHU e Internet así como: cortafuegos de red, antivirus de red, sistemas de detección de ataque distribuido (anti DDoS), sistemas de prevención de intrusiones (IPS), etc , .

La UPV/EHU, mediante los sistemas de seguridad para tal fin, podrá hacer uso de los datos registrados por estos elementos para el seguimiento y control del correcto funcionamiento de la red, sistemas, y servicios expuestos por esta y para salvaguardar la información albergada en ella.

La utilización de estos registros se realizará de acuerdo a las garantías establecidas en el artículo 87 de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. RESPONSABILIDADES

Todas las personas usuarias de la UPV/EHU, son responsables de conocer las normas que afectan al desarrollo de sus funciones, así como de las consecuencias en que pudieran incurrir en caso de incumplimiento.

4.1 RESPONSABILIDADES DE LAS PERSONAS USUARIAS

- Toda persona usuaria con acceso a internet es responsable del acceso y uso que haga de internet

- Las personas usuarias que se conectan a la red de datos corporativa se comprometen a respetar la configuración de los ordenadores corporativos suministrados por la UPV/EHU, empleando únicamente los programas instalados por los servicios informáticos de la UPV/EHU.

- Las personas usuarias de la comunidad universitaria que utilicen recursos externos deberán ajustarse a los criterios establecidos por las instituciones que proveen el servicio, la red, etc. Cuando se utilicen recursos de la UPV/EHU para acceder a otras redes, se deberán seguir en todo momento las normas establecidas para esas redes.

4.2 RESPONSABILIDADES DE LA UPV/EHU

- Disponer y mantener los recursos tecnológicos necesarios para el acceso adecuado a Internet.

- Velar por que las personas usuarias utilizan los servicios de internet de acuerdo con la reglamentación institucional y respetando las normas vigentes.

- Establecer las sanciones que podrán imponerse por el mal uso de Internet.

- Limitar el acceso a aquellos sitios que considere inadecuados basándose en el código de ética aprobado por el UPV/EHU.

5. INCUMPLIMIENTO DE LA NORMATIVA

Constatado un incumplimiento de la Normativa de Seguridad de la Información de la UPV/EHU, instará por los cauces establecidos en los Estatutos de la UPV/EHU, la depuración de las responsabilidades disciplinarias a las que hubiera lugar.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del alumnado y/o personal al servicio de las Administraciones Publicas o de la propia UPV/ EHU.

6. REVISIÓN Y EVALUACIÓN

La gestión de esta Normativa de Seguridad corresponde al Comité de Seguridad de la UPV/EHU, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.

- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

- Verificar su efectividad.

Si existen circunstancias que así lo aconsejen, se revisará la presente Normativa de Seguridad, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad de la UPV/EHU.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad de la Información el encargado de la custodia y divulgación de la versión aprobada de este documento.

7. REFERENCIAS

- **Internas:**
  - Política de Seguridad de la Información aprobado por el Consejo de Gobierno del 21 de Marzo de 2013:
    https://www.euskadi.eus/web01-bopv/es/bopv2/datos/2013/05/1302239a.shtml

  - https://www.ehu.eus/es/web/gardentasun-ataria/etika-kodearen-proposamena

- **Externas:**
  - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Versión	Aprobada el:
1.0	20 de noviembre de 2024