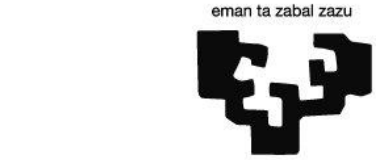

Normativa permisos de administrador en equipos de usuario UPV/EHU

Índice

1. Introducción.

En cumplimiento a la normativa actual de la UPV/EHU en materia de seguridad de la Información (https://www.ehu.eus/es/web/ikt-tic/normativas-de-seguridad-tic) y a los principios establecidos por el **Esquema Nacional de Seguridad (ENS)**, y con el objetivo de garantizar la integridad, disponibilidad y confidencialidad de los sistemas de información, de forma general **no se otorgarán permisos de administrador local a los usuarios sobre los equipos informáticos**.

2. Ámbito de aplicación.

La presente normativa es de aplicación a todo el ámbito de actuación de la UPV/EHU, y sus contenidos derivan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la UPV/EHU. Esta normativa y derivadas se aplicará a todo "equipo informático de usuario propiedad de la UPV/EHU".

La presente normativa ha sido aprobada por el comité de Seguridad TIC de la UPV/EHU.

3. Normativa a aplicar.

De acuerdo con el principio de **mínimos privilegios** recogido en el ENS, los usuarios dispondrán exclusivamente de los permisos necesarios para el desarrollo de sus funciones. El acceso con privilegios elevados se limitará al personal técnico autorizado y debidamente acreditado para la gestión, mantenimiento y soporte de los sistemas.

Esta medida contribuye a minimizar los riesgos asociados a la instalación de software no autorizado, la alteración indebida de configuraciones de seguridad y la posible exposición a amenazas de seguridad, garantizando un entorno tecnológico controlado y alineado con las medidas de protección requeridas.

Cualquier excepción a esta restricción deberá estar debidamente justificada y documentada, y requerirá la aprobación expresa del Responsable de Seguridad, conforme al procedimiento establecido por la organización. En estos casos, se contemplará la posibilidad de delegar temporalmente dicha responsabilidad bajo condiciones estrictamente controladas y con supervisión continua. A continuación, se detallan los escenarios específicos en los que podría considerarse dicha excepción:

3.1. Permisos para personal TIC y equipos de uso general

En aquellas situaciones en las que el personal de los servicios TIC de centros o departamentos —exceptuando al personal del área de atención a usuarios, que ya dispone de los permisos correspondientes— que deban usar equipos de uso compartido (como proyectores o dispositivos en salas de reuniones) requieran la

instalación de software específico para el desarrollo de presentaciones u otras actividades programadas, podrá autorizarse la concesión temporal de permisos con privilegios elevados.

Esta medida tiene como objetivo evitar la dependencia directa del Centro de Atención al Usuario (CAU) y prevenir retrasos que puedan comprometer la correcta ejecución de las actividades previstas.

Será imprescindible que el software a instalar cuente con la correspondiente licencia, esté debidamente verificado y cumpla con los requisitos legales y de seguridad establecidos por la organización.

3.2 Permisos para personal de investigación

Desde la Vicegerencia de las Tecnologías de la Información y la Comunicación (VGTIC), se recomienda encarecidamente el uso de **máquinas virtuales** en los propios equipos de trabajo como entorno aislado para la realización de pruebas e instalaciones de software. Esta medida permite que el usuario disponga de los privilegios necesarios sin comprometer la **integridad, disponibilidad y confidencialidad** del equipo ni de la información que en él se gestiona.

No obstante, somos conscientes de que pueden existir limitaciones técnicas o legales —como restricciones de licenciamiento o requisitos específicos del software— que dificulten el uso de entornos virtualizados. Por ello, se establecen a continuación distintas casuísticas en las que la concesión de permisos de administración podrá contemplarse de forma diferenciada:

3.2.1 Usuarios en estancias fuera de la UPV/EHU

En el caso de personal en estancias oficiales fuera de la universidad, se podrá solicitar la **concesión temporal de permisos de administrador local**. La solicitud deberá ser tramitada a través del **Centro de Atención al Usuario (CAU)**, y los permisos se otorgarán únicamente por el tiempo imprescindible para el desarrollo de la actividad. En ningún caso se concederán con carácter indefinido.

3.2.2 Personal docente e investigador con requerimientos técnicos específicos

Para usuarios cuya actividad profesional implique, de forma recurrente, la instalación y desinstalación de software —como es el caso del **personal docente e investigador** en los ámbitos de la **Informática, Telecomunicaciones y disciplinas**

afines—, se podrá autorizar el acceso con privilegios de administración sobre su equipo, siempre que se cumplan las siguientes condiciones:

- El usuario deberá comprometerse formalmente a seguir las directrices y buenas prácticas establecidas por la VGTIC (ver **Anexo 1**).
- En caso de detectarse comportamientos anómalos o incumplimiento de las medidas de seguridad por parte de los sistemas de protección de la UPV/EHU, dichos permisos podrán ser **revocados de manera inmediata y sin previo aviso.** Dicha revocación será debidamente notificada a la persona usuaria a través de los canales oficiales de comunicación, tales como el correo electrónico institucional o mediante contacto telefónico.

Esta flexibilización responde a la necesidad de **evitar el uso de equipos no gestionados por la UPV/EHU** para fines de investigación, lo cual supondría un riesgo considerable al no contar con las medidas de seguridad establecidas institucionalmente.

3.3 Equipos de aulas docentes.

En aquellos equipos ubicados en aulas docentes en los que, por necesidades derivadas de prácticas académicas, los estudiantes o el personal docente e investigador requieran permisos de administrador, dichos permisos podrán ser concedidos previa solicitud al personal técnico del centro responsable de la gestión de dichos equipos.

La validación de acceso en estos equipos deberá realizarse mediante el sistema de autenticación corporativo (Active Directory). El procedimiento de escalado de privilegios se efectuará utilizando mecanismos seguros: mediante `sudo` en sistemas Linux, o bien a través de permisos especiales en sistemas Windows, exigiéndose siempre la introducción de la contraseña correspondiente como parte del proceso de validación.

3.4 Casos en los que no se concederán permisos de administrador

Se denegará la concesión de permisos con privilegios elevados en los siguientes casos:

- **Equipos asignados a cargos directivos dedicación exclusiva**: A los usuarios con dedicación exclusiva en funciones de dirección o gestión no se les concederán permisos de administración local, dado que no se justifica su necesidad operativa.
- **Usuarios cuyo vínculo contractual no contemple funciones técnicas**: No se autorizarán permisos a aquellos perfiles cuyo contrato con la UPV/EHU no

incluya funciones relacionadas con la instalación, prueba, desarrollo o gestión de software informático.

4. Responsabilidades

Todos los usuarios tienen la obligación de colaborar con la UPV/EHU para corregir, cesar y, en su caso, rectificar el ejercicio de acciones que incumplan esta normativa.

Aquellas personas que, de forma reiterada, deliberada o por negligencia ignoren o infrinjan la presente normativa, podrán verse sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) que se estimen oportunas.

Constatado un incumplimiento de las obligaciones derivadas de esta normativa, el Comité de Seguridad de la Información podrá instar 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 de estudiantes, del personal al servicio de las Administraciones Públicas o de la propia UPV/EHU.

5. Revisión y evaluación

La gestión de esta Normativa de Seguridad corresponde al Comité de Seguridad de la información 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, al visto bueno 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 de la UPV/EHU el encargado de la custodia y divulgación de la versión aprobada de este documento.

6.Glosario

- **Software verificado:** Se entiende por software verificado aquel del que se posee una licencia legal de uso, ya sea mediante pago o bajo una modalidad de uso libre, con pleno conocimiento y cumplimiento de las condiciones que regulan su utilización. Además, debe haber sido sometido a un análisis de seguridad, como por ejemplo mediante herramientas como VirusTotal, para garantizar que está libre de software malicioso.

- **Software no autorizado:** Se considera software no autorizado aquel que se instala, utiliza o distribuye sin contar con la correspondiente licencia legal o sin el consentimiento explícito de la organización responsable del entorno donde se ejecuta. También incluye cualquier aplicación que no esté relacionada con las funciones académicas, administrativas o de investigación del usuario. Esto abarca programas de origen desconocido sin verificación de seguridad.

- **Equipo de usuario**: Se refiere a los dispositivos tecnológicos utilizados directamente por una persona para realizar tareas informáticas o digitales. Son las herramientas que emplea el usuario final para acceder a servicios, aplicaciones, redes o contenidos. Ejemplos: Ordenador portátil o de sobremesa, tabletas, smartphones, ...

- **Equipo informático**: Es un término más amplio que incluye todos los dispositivos y sistemas que forman parte de una infraestructura tecnológica, tanto para el uso individual como para el funcionamiento general de una red o sistema de información. Ejemplos: Servidores, equipos de red, sistemas de almacenamiento, equipos de usuario.

7.Referencias

Internas:

- Política de Seguridad de la Información aprobado por el Consejo de Gobierno del 21 de marzo de 2013: http://www.idazkaritza-nagusia.ehu.es/p254-content/es/contenidos/normativa/normativa_upvehu/es_norupv/adjuntos/Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

Externas:

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

Anexo I

Concesión de permisos de administrador en el equipo asignado al usuario

Por medio del presente documento, se concede al usuario **[Nombre del Usuario]** permisos de administrador en el equipo informático [Código equipo VGTIC]. Esta concesión queda condicionada al cumplimiento estricto de las siguientes medidas de seguridad y normas de uso, conforme a las directrices establecidas por la Vicerrectorado de Gestión de las Tecnologías de la Información y la Comunicación (VGTIC):

Condiciones de uso y seguridad

- **Identificación del usuario en el equipo**
  El equipo en la medida de los posible deberá estar en el dominio (AD) de la UPV/EHU para poder realizar el acceso al mismo usando las credenciales LDAP de la UPV/EHU.
  - En caso de no ser viable, se utilizará la cuenta LDAP de la UPV/EHU o la cuenta de correo electrónico institucional del usuario para poder tener trazabilidad con las herramientas de ciberseguridad de las acciones realizadas usando la cuenta del usuario.
- **Instalación obligatoria de herramientas de seguridad**
  El equipo deberá contar con las soluciones de seguridad que determine la VGTIC, con el fin de garantizar su protección y permitir su gestión remota. Estas incluyen, entre otras:
    - Antivirus
    - Protección contra ransomware
    - Soluciones EDR/XDR
    - Herramienta de gestión remota (ejmp: Ivanti, Intunes, etc)

Nota: Aunque algunas de estas soluciones están disponibles únicamente para entornos Windows, en cuanto existan versiones compatibles con otros sistemas operativos, deberán ser igualmente instaladas.

- **Sistema operativo recomendado**
  Se recomienda el uso de equipos con sistema operativo Windows 11 o el recomendado por la VGTIC en las imágenes corporativas. En aquellos casos en que se requiera el uso de Linux, se priorizará el uso de las funcionalidades de integración de Linux en Windows (WSL – Windows Subsystem for Linux).
- **Gestión de incidentes de seguridad**
  En caso de detectarse un incidente de seguridad relacionado con el equipo, la VGTIC, previa autorización del responsable de seguridad y notificación al Comité de Seguridad, podrá proceder al aislamiento del equipo, su bloqueo o

cualquier otra medida necesaria, hasta la resolución del incidente junto con el usuario responsable.

- **Licenciamiento del software**
  Solo podrá utilizarse software legal y debidamente licenciado. Queda prohibido el uso de software no autorizado o que infrinja derechos de propiedad intelectual.

- **Administración compartida del equipo**
  La administración del equipo será compartida entre el usuario y la VGTIC. Esta última se reserva el derecho de:

  a) Instalar software que, por motivos institucionales, de servicio o de seguridad, deba estar presente en todos los equipos de la UPV/EHU.
  b) Desinstalar software que interfiera con el funcionamiento del software institucional o comprometa la seguridad del equipo. En este caso, será debidamente notificada a la persona usuaria a través de los canales oficiales de comunicación, tales como el correo electrónico institucional o mediante contacto telefónico.

- **Restricciones del usuario**
  - El usuario **no podrá desinstalar** ningún software previamente instalado por la VGTIC en el equipo.
  - El usuario deberá respetar las cuentas y grupos creados en los equipos y sus permisos asociados, es decir, quedará totalmente prohibido la modificación o creación de cuentas o grupos privilegiados o no en el equipo.

Este documento debe ser aceptado por el usuario como condición indispensable para la concesión de permisos de administración local en su equipo.

Versión	Aprobada el:
1.0	7 de julio de 2025