

INSTRUCCIONES DE USO DE LOS SISTEMAS Y RECURSOS DIGITALES POR PARTE DEL ESTUDIANTADO DEL CENTRO UNIVERSITARIO

Aprobadas per la Comisión Permanente en fecha 5 de marzo de 2026

Artículo 1. Objeto

1.1. Estas instrucciones tienen por objeto regular el uso correcto, responsable y seguro de los sistemas de información y recursos digitales de la Fundación TecnoCampus por parte de los y las estudiantes.

1.2. La finalidad de estas instrucciones es garantizar la seguridad de la información, proteger los activos tecnológicos del centro, asegurar un uso responsable y adecuado de los recursos digitales y prevenir incidentes de ciberseguridad.

Artículo 2.- Ámbito de aplicación

2.1. Esta instrucción se aplica a todos los y las estudiantes matriculadas en estudios oficiales o propios de la Fundación TecnoCampus que dispongan de acceso a los sistemas y recursos digitales del centro, incluyendo: la cuenta de correo electrónico institucional, el campus virtual, la red WI-FI, equipos y aulas de informática, así como plataformas o servicios en línea proporcionados por el centro.

2.2. Esta instrucción será igualmente aplicable a cualquier otro sistema, herramienta o servicio digital que TecnoCampus pueda poner a disposición de los estudiantes en el futuro.

Artículo 3.- Principios generales de uso

3.1. Los sistemas y recursos digitales de TecnoCampus deben ser utilizados:

- a) Con fines académicos o relacionados con la condición de estudiante.
- b) De manera responsable, respetuosa y conforme a la normativa vigente.
- c) Sin poner en riesgo la seguridad, disponibilidad o integridad de los sistemas o de la información.

Artículo 4.- Credenciales y acceso a los sistemas

4.1. Debe tenerse en cuenta que:

- a) La cuenta institucional es personal e intransferible.
- b) Está prohibido compartir credenciales de acceso (usuario y contraseña) con terceras personas.
- c) El o la estudiante es responsable de todas las actividades que realice con su cuenta.
- d) Deben utilizarse contraseñas robustas y mantenerlas confidenciales.
- e) Cualquier sospecha de acceso indebido, suplantación de identidad o intento de phishing debe comunicarse inmediatamente al SIT: sit@tecnocampus.cat

4.2. TecnoCampus puede suspender temporalmente el acceso a los sistemas en caso de riesgo para la seguridad.

Artículo 5. Usos permitidos

5.1. Los y las estudiantes pueden utilizar los recursos digitales:

- a) Para la realización de actividades docentes y de aprendizaje.
- b) Para la comunicación con el profesorado, los servicios administrativos y otros miembros de la comunidad universitaria.
- c) Para la gestión de trámites académicos.
- d) Para otras actividades vinculadas a su condición de estudiante.
- e) En general, para la realización de cualquier actividad académica que no contravenga estas instrucciones.

Artículo 6. Usos y actividades no permitidos

6.1 Queda expresamente prohibido:

- a) Acceder sin autorización a cuentas, sistemas o información de otros usuarios.
- b) Intentar vulnerar la seguridad de la red o de los sistemas del centro.
- c) Utilizar técnicas de intrusión o hacking.
- d) Suplantar la identidad de otras personas.
- e) Difundir malware, virus o contenido malicioso.
- f) Enviar correo basura o comunicaciones masivas.
- g) Utilizar sistemas con fines comerciales o lucrativos sin autorización expresa.
- h) Compartir contenidos ilegales o que vulneren derechos de propiedad intelectual.
- i) Manipular las cabeceras de los mensajes de correo para ocultar al autor o el origen.
- j) Hacer un uso que perjudique el funcionamiento normal de los servicios tecnológicos del centro.
- k) Cualquier uso que implique una actuación delictiva, deshonesta o no ética.
- l) Difundir o crear contenidos falsos o manipulados (“fake news”), así como contenidos alterados mediante técnicas de manipulación digital o audiovisual (incluyendo “deep fake”), que puedan inducir a error, perjudicar a terceros o dañar la reputación de personas o instituciones.

Artículo 7. Uso de herramientas de inteligencia artificial

7.1. El uso de herramientas de inteligencia artificial debe realizarse de manera responsable y ética, conforme a la normativa vigente y a las directrices que establezca el centro o el profesorado en el marco de la actividad académica.

7.2. Los y las estudiantes son responsables del uso que hagan de estas herramientas y del contenido que resulte de las mismas, así como del cumplimiento de la normativa académica aplicable, de propiedad intelectual, protección de datos y uso de los sistemas de información.

7.3. El uso de esta tecnología no podrá comportar riesgos para la seguridad de los sistemas, la confidencialidad de la información ni para los derechos de terceros.

Artículo 8. Campañas de seguridad y simulaciones de phishing

8.1. Con la finalidad de mejorar la ciberseguridad y el nivel de concienciación digital, TecnoCampus puede llevar a cabo acciones de formación, campañas de sensibilización y simulaciones de phishing (phishing simulado o ético) con finalidades preventivas y educativas, orientadas a mejorar la seguridad digital de la comunidad universitaria.

8.2. Estas actuaciones no tienen finalidad sancionadora, sino únicamente preventiva.

8.3. Los datos obtenidos en el marco de estas acciones podrán ser analizados con fines de mejora de los sistemas de seguridad y, en su caso, con fines de investigación, siempre de manera agregada y anonimizada, de acuerdo con la normativa vigente en materia de protección de datos.