CEADE
SAN ISIDORO
CENTRO UNIVERSITARIO

CÓDIGO DE CONDUCTA DIGITAL

Normas de uso responsable de los recursos tecnológicos

Declaración de principios. *Los recursos digitales e informáticos que el Centro pone a disposición de su comunidad son herramientas exclusivas para el desarrollo de la actividad docente, investigadora y administrativa. Su uso debe regirse siempre por los principios de responsabilidad, respeto, legalidad y seguridad de la información*

1. Uso del correo electrónico corporativo

- Identidad profesional. El correo electrónico corporativo es el único canal online oficial de comunicación académica y administrativa. Debe utilizarse exclusivamente para fines relacionados con el Centro.
- Seguridad. Se debe activar y mantener el Doble Factor de Autenticación (MFA) para proteger el acceso a la cuenta. Las credenciales son personales e intransferibles.
- Restricciones de uso. Queda prohibido utilizar la dirección institucional para registrarse en plataformas web, foros o servicios de carácter personal ajenos al ámbito universitario, así como el envío masivo de correos no autorizados (SPAM).

2. Campus virtual y almacenamiento cloud

- Garantía de privacidad en la nube. Toda la documentación académica y de gestión debe almacenarse de manera obligatoria en las unidades oficiales de Google Drive designadas por la organización. Queda prohibido guardar información institucional o datos personales sensibles en cuentas personales externas o en discos locales no cifrados.
- Propiedad intelectual de los recursos. Los materiales docentes, exámenes, presentaciones, trabajos, videoclases, podcast, materiales y apuntes alojados en el campus virtual son propiedad del centro y sus autores. Queda estrictamente prohibido descargarlos para su distribución, venta o publicación en redes sociales o plataformas externas de apuntes sin autorización previa por escrito.
- Respeto al derecho de cita. Al incorporar material ajeno en trabajos académicos y presentaciones docentes, se debe respetar el derecho de cita, mencionando al autor y la fuente original.

3. Equipamiento y redes del centro

- Deber de salvaguarda. Al ausentarse de cualquier puesto de trabajo, despacho o aula de informática, el usuario debe bloquear la pantalla del ordenador mediante contraseña para evitar cualquier uso o acceso no autorizado.
- Integridad de los equipos. No se permite la instalación de software no licenciado, herramientas de intercambio P2P o configuraciones de red que puedan comprometer la seguridad perimetral del centro.
- Protección contra amenazas. Queda prohibido introducir, ejecutar o difundir virus, troyanos o cualquier otro tipo de código malicioso o secuencia de comandos que puedan dañar, manipular o alterar los sistemas del centro o de terceros.
- Uso consecuente de la red. Se prohíbe realizar un consumo masivo o abusivo de los recursos de red y servidores que pueda obstaculizar o interrumpir el acceso al servicio del resto de usuarios de la comunidad.

4. Gestión de incidentes y consecuencias

- Notificación inmediata. Ante cualquier sospecha de brecha de seguridad (pérdida de credenciales, infección por malware o extravío de equipos corporativos), el usuario tiene la obligación de reportarlo al Área de Informática y al Delegado de Protección de Datos (datos@centrosanisidoro.es) en un plazo máximo de 24 horas desde su detección.
- Régimen sancionador. El uso indebido de los recursos tecnológicos o la vulneración de las medidas de seguridad lógicas del centro dará lugar a las responsabilidades disciplinarias o medidas académicas correspondientes bajo las normas de convivencia del Centro Universitario San Isidoro o la legislación laboral vigente, sin perjuicio de las posibles responsabilidades civiles o penales derivadas.