COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

TÉRMINOS Y CONDICIONES DE USO DE LOS SISTEMAS DE INFORMACIÓN

Normas y buenas prácticas para un uso responsable y seguro de los recursos digitales de la Universidad, aplicables a PDI, PAS, Alumnado y Terceros contratados. Incluye pautas de seguridad y criterios de actuación ante incidentes e incumplimientos.

ciberseguridad.comillas.edu

RESUMEN EN 5 MINUTOS

¿Por qué es necesaria esta normativa?

Objetivo Principal: garantizar la integridad de la información y fomentar un entorno de respeto entre todos los miembros de la comunidad universitaria.

Responsabilidad Compartida: la seguridad no es solo tecnología; es el comportamiento de cada usuario. La imprudencia o negligencia puede derivar en graves consecuencias, incluida la responsabilidad civil y penal.

Meta: priorizar la educación y la sensibilización para prevenir riesgos.

La seguridad es tarea de todos.

A quién aplica y qué protegemos

Usuarios

- PAS
- PDI
- Estudiantes
- Proveedores externos

Términos y condiciones de uso

Sistemas

- Hardware y software (aulas/despachos)
- Redes y conectividad (WiFi/VPN)
- Dispositivos personales /BYOD)
- Nube y almacenamiento
- IoT y pantallas conectadas

Comunicaciones electrónicas: identidad y buen uso

SÍ HACER

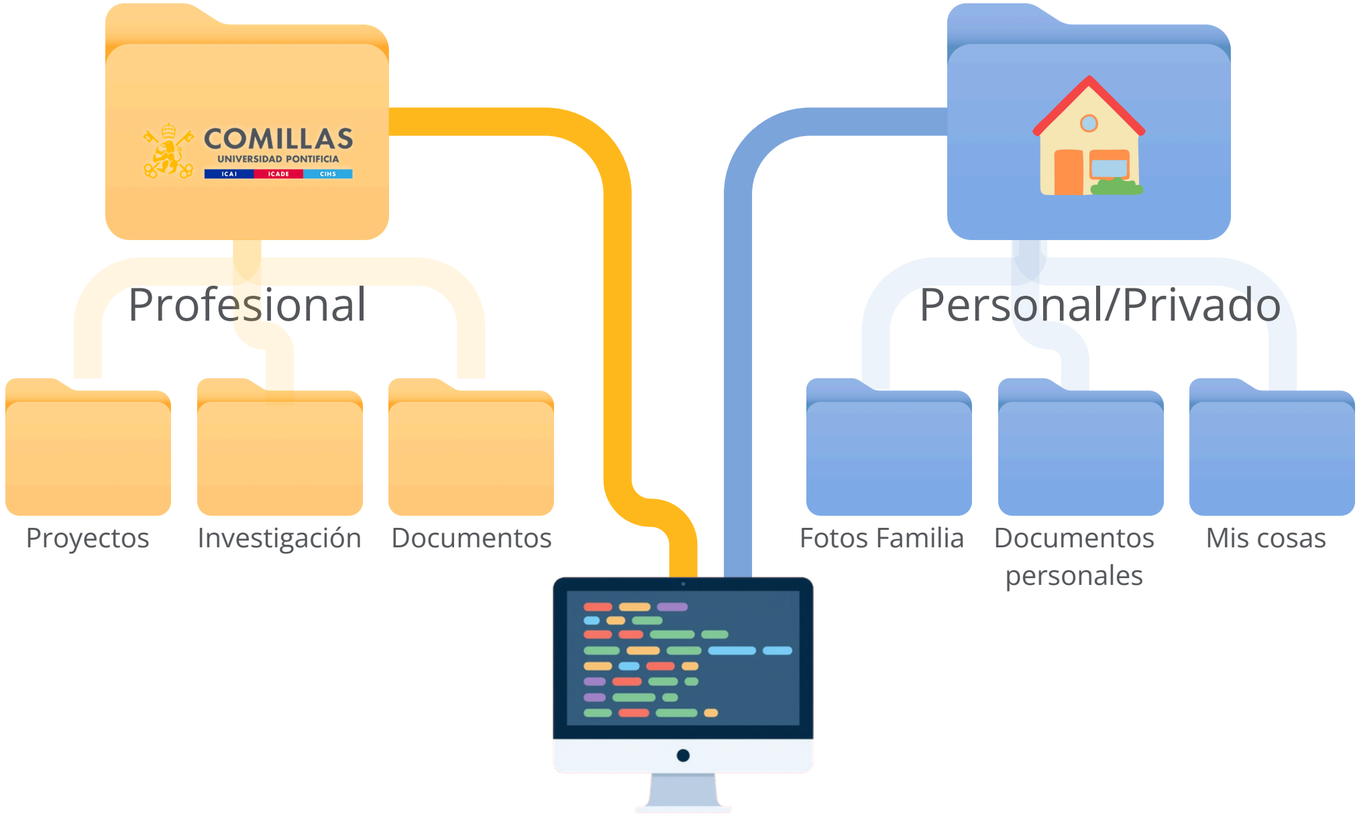
- Usar para **fines académicos, administrativos** y de **investigación.**
- **Verificar** siempre el remitente antes de abrir adjuntos.
- **Proteger** la **identidad institucional** (personal e intransferible).

NO HACER

- **Enviar correo no solicitado** (SPAM) o cadenas masivas.
- **Difundir contenidos inapropiados**, ofensivos o difamatorios.
- **Suplantar la identidad** de otros usuarios.

Cada correo institucional que envías puede afectar a la seguridad, la reputación y la confianza en la Universidad.

Datos personales VS datos profesionales



El usuario es el único responsable de realizar copias de seguridad de sus datos personales.

Reglas de oro

1. **Identificación:** la información privada debe estar separada y claramente identificada (ej.: carpeta PERSONAL).
2. **Almacenamiento:** los datos de la universidad **NO** deben guardarse en nubes personales (Google Drive, Dropbox) sin permiso.
3. **Limpieza:** el usuario es responsable de borrar sus datos privados al finalizar su relación con la Universidad.

Principios básicos de ciberseguridad

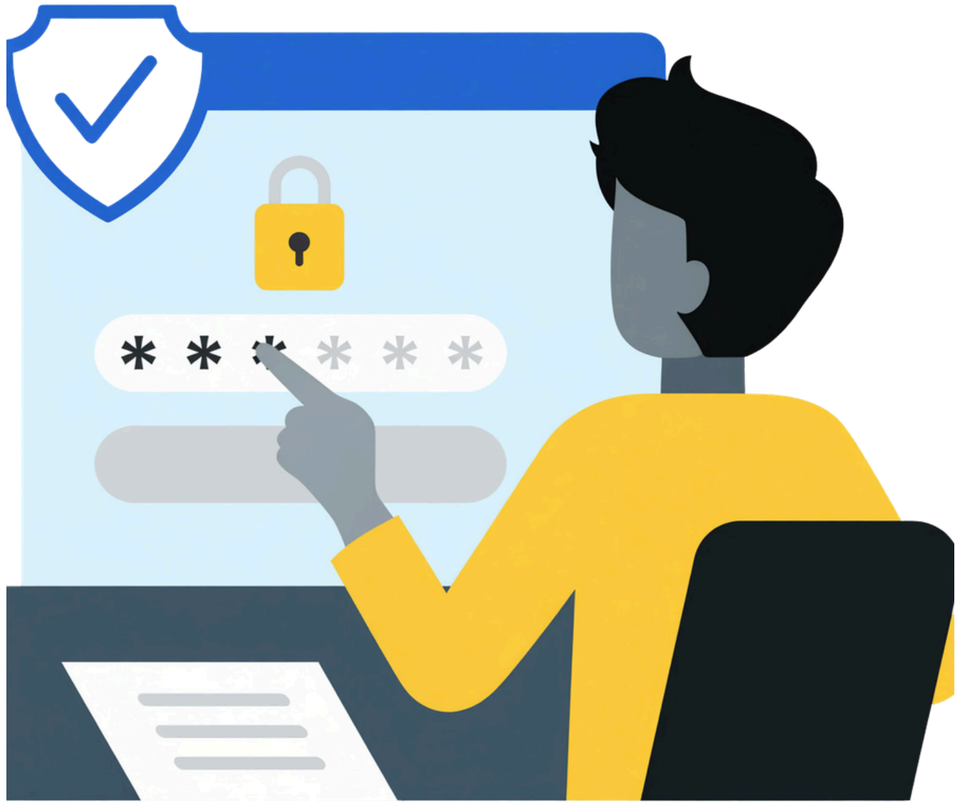
Software legal:
solo usar software autorizado. Prohibido terminantemente el software pirata.

Actualizaciones:
mantener actualizadas las aplicaciones externas para cubrir brechas de seguridad.

Dispositivos personales:
si usas la red o VPN, tu equipo debe tener antivirus actualizado y clave robusta.

Vigilancia:
reporta los mensajes de phishing desde el menú **INICIO,** haz click en **Informar sobre correo de pishing.**

Política de contraseñas y accesos



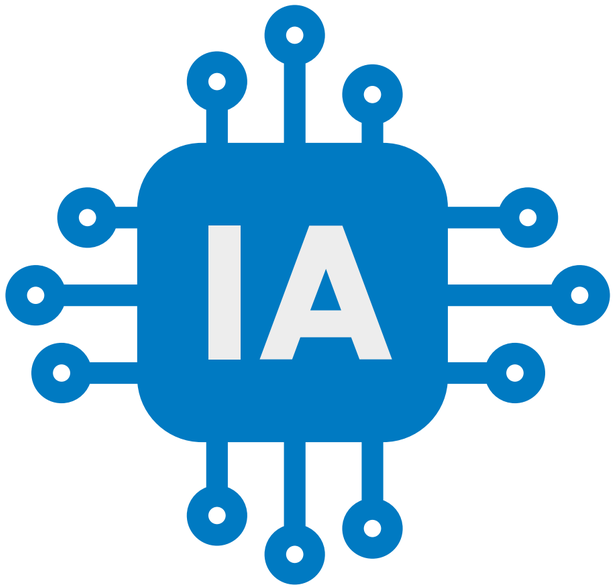
- Longitud: **mínimo 10 caracteres.**
- Complejidad: mezclar **mayúsculas, minúsculas, números y símbolos.**
- Rotación: **obligatorio cambiar anualmente** (o antes si hay indicios de compromiso).
- **Doble Factor (2FA)**: obligatorio configurar a primer acceso (app o token).

PROHIBIDO

- Anotar claves en post-its o archivos de texto.
- Compartir contraseñas con compañeros.
- Reutilizar contraseñas personales.

Inteligencia artificial: límites y precauciones

Datos confidenciales:
PROHIBIDO introducir datos personales o restringidos en IAs públicas (ej.: ChatGPT)



Código fuente:
no subir código de la Universidad en IAs externas sin supervisión.

Verificación humana:
los resultados de la IA pueden tener errores. Revisión obligatoria.

Herramientas:
usar soluciones aprobadas. Para nuevas herramientas, solicitar vía Jira al STIC.

Acceso a Internet y redes privadas

Navegación y VPN oficial

El acceso se realiza a través de sistemas de seguridad filtrados. Uso exclusivo del servicio VPN oficial de la Universidad.

Redes anónimas y VPNs externas

Prohibido el uso de la red TOR y VPNs no autorizadas debido a la imposibilidad de garantizar la seguridad y el control.

El usuario es el **único responsable de la custodia y uso** de sus credenciales de acceso.

Protección de datos y privacidad (RGPD)

Cifrar todos los datos personales

Clasificación: etiquetar siempre la información (pública, interna, confidencial, restringida).

Minimización: no recolectar más datos de los necesarios. Anonimizar cuando sea posible.

Notificación: todo nuevo tratamiento de datos debe notificarse al Delegado de Protección de Datos: **dpo@comillas.edu**

Derechos ARCO: para ejercer derechos, contactar a **prodatos@comillas.edu**
(Acceso, rectificación, supresión, etc.)

Propiedad intelectual y licencias

Licencias de software: respetar estrictamente las licencias adquiridas. Prohibida la copia o distribución ilegal.

Propiedad institucional: toda información, documento o código creado con cuentas profesionales es propiedad de la Universidad.

Derechos de autor: no reproducir textos o imágenes protegidas sin autorización escrita.

Uso no comercial: los recursos son exclusivamente para fines académicos y administrativos.

Trazabilidad y monitorización

Concepto:
el sistema guarda registros (logs) de quién, cuándo y qué se hace en la red.

Propósito de la monitorización:

- Detectar incidentes de seguridad y abusos.
- Optimizar el rendimiento de recursos.
- Cumplimiento legal.

Garantía:
el personal técnico que accede a estos datos está sujeto a un estricto deber de confidencialidad.

Usuarios externos y contratistas

Solicitud en Jira

Responsable solicita alta, iindicando fechas.

Contrato y claúsulas

Inclusión de aceptación de normativa.

Cumplimiento

Los externos son una extensión de la comunidad y siguen las mismas normas.

Revocación

Baja automática al fin del contrato.

Incumplimiento y sanciones

El incumplimiento se considera una violación grave de las políticas.

Medidas técnicas

- Restricción de acceso.
- Bloqueo de privilegios.

Medidas disciplinarias

- Sanciones según RRHH (PAS/PDI)
- Terminación de contrato (externos).

Responsabilidad legal

- Posible responsabilidad civil o penal según legislación vigente.

Resolución: RRHH, Asesoría Jurídica y STIC determinarán la gravedad.

Resumen y contactos clave

Checklist digital

- Usa contraseñas fuertes y 2FA.
- No compartas datos sensibles en IAs.
- Separa tu vida digital personal de la profesional.
- Reporta cualquier actividad sospechosa.

Incidentes de seguridad:
ciberseguridad@comillas.edu

Protección de datos (DPO):
dpo@comillas.edu

Soporte técnico:
Portal JIRA STIC