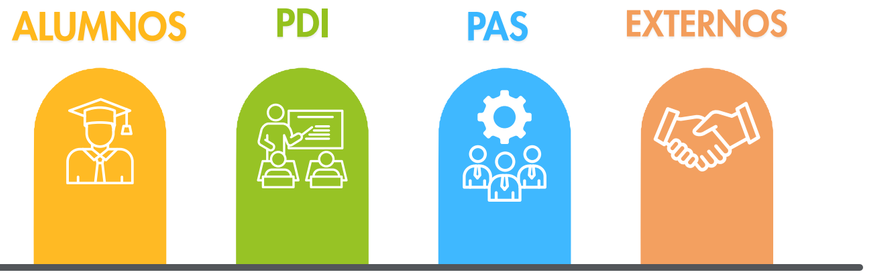
COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Resumen de referencia
Versión 1.0



La información es un activo estratégico

El objetivo es minimizar el riesgo y garantizar la calidad de los servicios. La seguridad es responsabilidad de todos los usuarios.

Confidencialidad

Acceso solo a personas autorizadas.

Disponibilidad

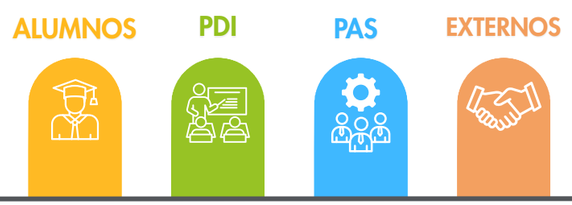
Acceso a la información en el tiempo y forma requeridos.

Integridad

Exactitud de los datos sin alteraciones no autorizadas.

Trazabilidad

Rastreo de accesos e intentos de acceso.



Alcance y perímetro de seguridad

La política se aplica integralmente a todo el Sistema de Información, sin importar la ubicación de los datos.

Clasificación de la información

Obligatorio para PAS y PDI

4 . Restringido

Altamente sensible. Acceso estrictamente limitado a un servicio (ej.: RRHH, STIC...)

3 . Confidencial

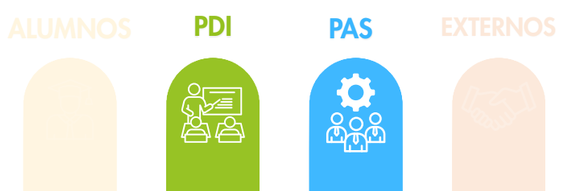
- Básico (valor moderado)
- Cifrado (datos sensibles financieros)
- Acceso limitado (temporal 30 días)

2 . Interno

Uso interno y propiedad intelectual (ej.: material pedagógico)

1 . Público

Acceso libre (ej.: publicaciones institucionales)



Protección de datos de carácter personal

Cumplimiento estricto del RGPD y normativa vigente

Confidencial - Cifrado

Nivel mínimo a aplicar en las herramientas de la Universidad para todos los datos personales.

Brechas de seguridad

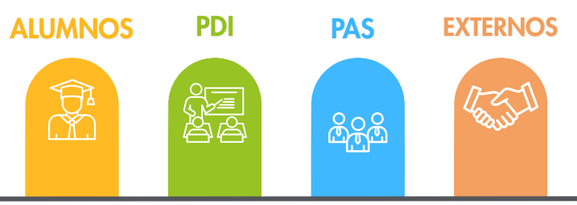
Debe comunicarse en un plazo máximo de 72 horas tras detectar una brecha de datos personales.

Minimización y anonimización

Conservar solo los datos personales necesarios y anonimizar o seudonimizar cuanto antes.

Evaluación de los riesgos

Contactar con el DPO (dpo@comillas.edu) lo antes posible al iniciar un proyecto con datos personales.



Principios de seguridad

Hábitos diarios para prevenir incidentes

Bloqueo de sesión

Siempre bloquear el equipo al ausentarse (Win+L)

Despacho limpio

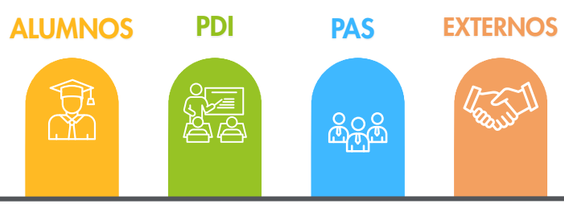
No dejar información sensible a la vista (papeles, pizarras) ni llaves puestas.

Copias de seguridad

Realizar respaldos diarios de los datos importantes

Control de acceso

No compartir credenciales ni dejar recursos abiertos.



Buenas prácticas de seguridad y uso de recursos: alumnos

COMILLAS UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

Resumen de obligaciones y recomendaciones para dispositivos y accesos

Software y propiedad intelectual

Se debe usar únicamente software con licencia válida en los sistemas de la Universidad y respetar estrictamente los derechos de propiedad intelectual asociados.

Bloqueo de sesión

Bloquea siempre tu sesión al alejarte de tu equipo, aunque sea por un breve instante, para evitar accesos no autorizadores en entornos compartidos.

Doble factor de autenticación (2FA)

Activa la autenticación de doble factor para añadir una capa extra de seguridad a todos los servicios y cuentas de la Universidad.

Redes WiFI públicas

Evita el uso de puntos de acceso WiFi públicos no seguros debido al alto riesgo de ataques de interceptación de datos (tipo man-in-the-middle).

Mantenimiento de dispositivos personales

Es responsabilidad del alumno mantener actualizados el sistema operativo, las aplicaciones y el antivirus en sus ordenadores y dispositivos personales.

Riesgo de *pishing*

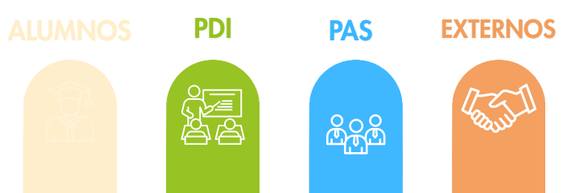
Presta atención a los correos sospechosos: pasa el cursor sobre los enlaces para verificar que dirigen a servicios oficiales de la Universidad y comprueba siempre la dirección del remitente, aunque recuerda que por sí sola no siempre es fiable.

ALUMNOS PDI PAS EXTERNOS

Seguridad en servidores y servicios

Gestión proactiva y mantenimiento seguro

- **Actualizaciones:** parches de seguridad y actualizaciones de sistema obligatorios.
- **Acceso seguro:** ningún recurso interno accesible desde el exterior sin VPN/Firewall.
- **Mantenimiento:** debe ser trazable, registrado y autorizado por el STIC.
- **Gestión de cambios:** evaluar impacto y planificar retorno antes de modificar infraestructura.



Política de copias de seguridad (backups)

Garantía de recuperación ante desastres o fallos

Frecuencia

Copias automáticas diarias para servidores y sistemas.

Pruebas

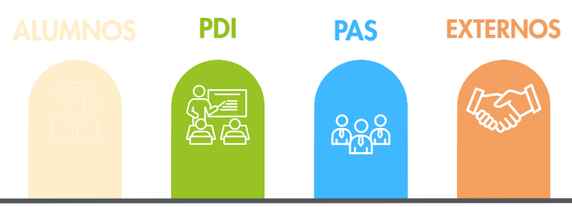
Validación regular de la restauración de datos.

Ubicación

Almacenamiento seguro y externalización semanal (off-site).

Alcance

Datos de usuario, aplicacines, bases de datos y configuraciones.



Seguridad del puesto de trabajo

El ordenador es la primera línea de defensa

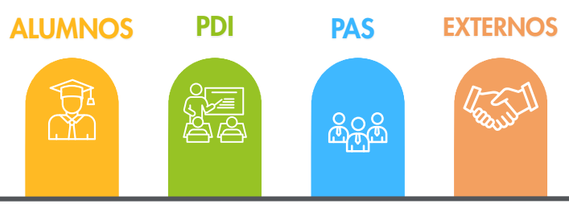
Reglas generales

Doble factor (2FA): obligatorio para cuentas de dominio.

Software Ilegal: estrictamente prohibido instalar software sin licencia o pirata.

Antivirus

- **Equipos Universidad:** gestionado y actualizado por el STIC.
- **Equipo Alumnos:** responsabilidad del alumno mantener su antivirus personal actualizado.



Movilidad y teletrabajo

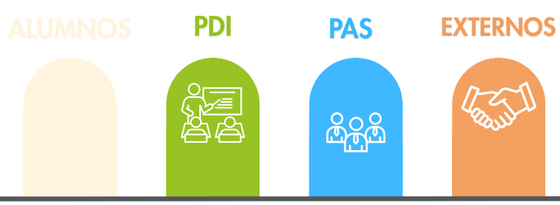
Mantener la seguridad fuera de las instalaciones de la Universidad

Conexión segura
Uso obligatorio de VPN de la Universidad para accesos remotos.

Entornos públicos
No trabajar con datos sensibles en trenes o estaciones (evitar miradas indiscretas).

Separación de uso
Diferenciar estrictamente entre uso profesional y personal.

Vigilancia
Nunca dejar dispositivos desatendidos.



Soportes extraíbles y correo electrónico

Precaución en el intercambio de información

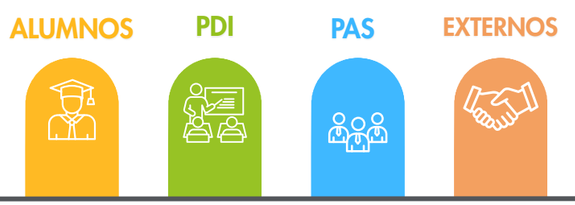
USB y discos externos

Deben estar cifrados si se utilizan para sacar datos de la Universidad.

Correo electrónico

Pishing: verificar siempre los remitentes.
Enlaces: pasar el ratón por encima (hover) para verificar la dirección real antes de hacer click.
Reporte: usar el botón dedicado para mensajes sospechos.

No conectar nunca memorias USB, tarjetas u otros dispositivos externos encontrados en aulas, buzones o lugares públicos para evitar la infección por malware y el robo de datos.



Responsabilidades y consecuencias

El cumplimiento de la política es obligatorio para todos los usuarios

Deber de confidencialidad

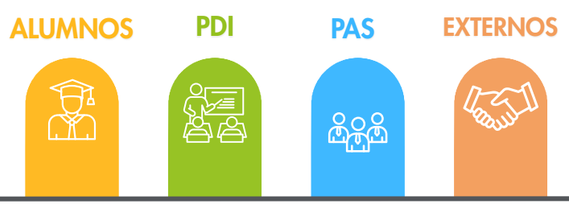
Obligación estricta de proteger la información

Sanciones

El incumplimiento puede derivar en acciones disciplinarias

Medidas de emergencia

El STIC puede revocar accesos o aislar equipos de forma inmediata ante amenazas graves



Gestión de incidentes de seguridad

Si detecta algo sospechoso, repórtelo inmediatamente

Notifica al Centro de Atención al Usuario

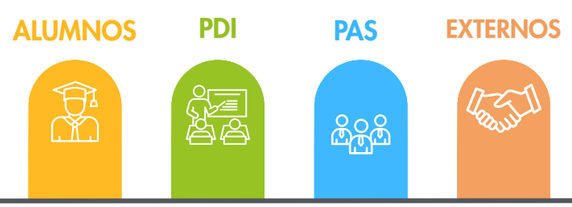
Utiliza los **canales** disponibles: teléfono, correo electrónico o Portal de Autoservicio.

El **objetivo** es contener el incidente y minizar daños.

Alerta: incluye fallos de seguridad, robo de credenciales o comportamiento anómalo.

Mails fraudulentos (phishing) o SPAM

- No respondas ni interactúes con el remitente
- Marca el mensaje como *phishing* en Outlook



Información adicional

Esta presentación es un resumen ejecutivo de la normativa vigente.

Para solicitar la versión completa de la Política de Seguridad de la Información **contacte a través del correo dop@comillas.edu**