NOTIFICAR UN INCIDENTE DE CYBERSEGURIDAD

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI | ICADE | CIHS

Esta guía ha sido diseñada con el objetivo de asegurar una gestión efectiva de los **incidentes de seguridad** y **proteger los recursos de información** de la Universidad Pontificia Comillas.
La colaboración y el compromiso de todos los miembros del personal y los alumnos son esenciales para mantener un entorno seguro y protegido.

IDENTIFICACIÓN DEL INCIDENTE

En nuestro contexto, un incidente se refiere a cualquier evento relacionado con la seguridad de la información que tenga un impacto negativo en los sistemas, servicios o datos de la Universidad. Tu vigilancia y reporte son esenciales para mantener un entorno seguro.

VIAS DE NOTIFICACIÓN

EN CASO DE **URGENCIA** (Teléfono):

Llame al **+34 91 542 28 00 ext 4444** si el incidente requiere atención inmediata.

INCIDENTE **DE FUGA DE DATOS:**

Ponte en contacto de inmediato con **dpo@comillas.edu**, Es un caso URGENTE.

INCIDENTE **NO URGENTE** (Ticket en Línea):

Utilice www.comillas.edu/**CAU-STIC** para todo tipos de incidentes que pueden esperar una respuesta programada.

NOTIFICACIONES **GENERALES** (Correo Electrónico):

Envíe detalles del incidente a ciberseguridad@comillas.edu.

COOPERACIÓN CON INVESTIGACIONES

Valoramos mucho la colaboración de los miembros de la comunidad universitaria en la investigación de incidentes. Apreciamos tu ayuda proporcionando información honesta y completa, evitando interferir en el proceso. Tu **cooperación es fundamental** para mantener un entorno seguro y positivo para todos.

CONFIDENCIALIDAD Y SEGURIDAD

Al reportar incidentes, ten en cuenta la importancia de mantener la **confidencialidad y seguridad de la información**. Evita compartir detalles que puedan poner en riesgo la investigación o la seguridad. Es esencial para proteger a todos los involucrados.

SEGUIMIENTO Y RESOLUCIÓN

Es fundamental que sigas las instrucciones del Servicio de Sistemas y Tecnologías de Información y Comunicaciones (STIC) y mantengas una comunicación constante hasta la resolución por completo el incidente. Tu colaboración es esencial para asegurar una rápida y efectiva solución.

NOTIFICAR UN INCIDENTE DE CYBERSEGURIDAD

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI | ICADE | CIHS

INCIDENTES QUE DEBEN NOTIFICARSE

1. Violaciones de Seguridad de Datos:
Acceso no autorizado a información sensible o confidencial. Fuga de datos personales de estudiantes o personal.
Es de vital importancia para poder tomar medidas rápidas y efectivas en la protección de la información personal. Tu pronta acción es fundamental para garantizar la seguridad de los datos.

2. Ataques Cibernéticos:
Ransomware o malware que afecta múltiples sistemas.
Ataques de denegación de servicio (DDoS) que interrumpen las operaciones de la universidad.

3. Compromiso de Cuentas:
Acceso no autorizado a cuentas de correo electrónico institucionales.
Sospecha de que una cuenta ha sido hackeada o está siendo usada para phishing.

4. Pérdida o Robo de Dispositivos:
Dispositivos institucionales con información sensible que han sido perdidos o robados.

5. Incidentes Legales y de Conformidad:
Violaciones de políticas de privacidad que puedan tener implicaciones legales.

INCIDENTES QUE NO REQUIEREN NOTIFICACIÓN

1. Problemas Técnicos Rutinarios:
Problemas menores de conectividad o hardware que no afectan la seguridad.
Fallos de software que no comprometen datos o la integridad del sistema.

2. Incidentes Aislados de Bajo Riesgo:
Pérdida de archivos no sensibles debido a errores no relacionados con la seguridad.
Errores ocasionales de aplicaciones que no comprometen la seguridad o los datos.

3. SPAM, Phishing y Correos Electrónicos No Solicitados Comunes:
Recepción de correos electrónicos no deseados que no contienen enlaces o archivos maliciosos. El botón "Informar sobre correo de phishing" está disponible para este fin en la pestaña superior "Inicio" de Outlook

Encuentre todos nuestros consejos de seguridad en: **ciberseguridad.comillas.edu**