UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

BOLETÍN INFORMATIVO

Gestión de los Sistemas de Información y las Telecomunicaciones

Volumen 3, número 8, septiembre de 2026

Protección de información Institucional

¿Por qué es importante proteger la información institucional?

Los ciberdelincuentes buscan obtener información institucional académica y administrativa, como proyectos, bases de datos, documentos financieros y datos personales, con el propósito de venderla, modificarla, divulgarla o solicitar rescates económicos.

¿Comó afecta la exposión o pérdida de información institucional?

La exposión o perdida de información afecta la confidencialidad, integridad y disponibilidad de los datos, generar interrupciones en los servicios institucionales y comprometer la confianza de comunidad universitaria.

¿Por qué representa un riesgo?

La Universidad Distrital administra grandes volúmenes de información sensible de carácter administrativo y académico, así como datos personales, que tienen alto valor para los grupos criminales.

¿Cómo operan los ciberdelincuentes?

Los atacantes emplean diversas técnicas para lograr su objetivo, entre las que se destacan:

- Envío de correos de phishing.
- Explotación de vulnerabilidades en aplicaciones.
- Uso de malware para robar credenciales.
- Uso de software malicioso.

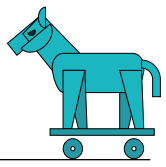
Señales de alerta

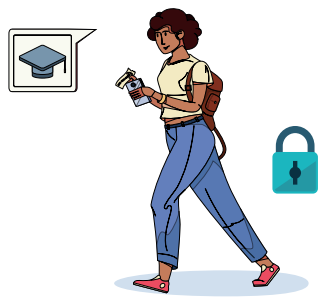
- Archivos que desaparecen o presentan modificaciones inesperadas.
- Accesos desde ubicaciones desconocidas.
- Solicitudes inesperadas para compartir documentos.
- Alertas de inicio de sesión en dispositivos desconocidos.

Una vez que obtienen acceso, extraen información sin ser detectados o permanecen dentro de la red universitaria durante largos periodos.

Buenas prácticas digitales

- Evitar compartir información sensible mediante aplicaciones personales
- Utilizar únicamente plataformas institucionales.
- Clasificar la información según su nivel de confidencialidad.
- Bloquear el equipo al ausentarse del puesto de trabajo.





Medidas preventivas

- Utilizar almacenamiento y espacios institucionales.
- Activar la autenticación multifactor (MFA).
- No compartir sus credenciales con nadie.

¿Sospechas? Si recibes un mensaje sospechoso o crees haber sido víctima:

1. No responda mensajes ni de clic en enlaces
2. Cambie inmediatamente su contraseña.
3. Reporte al área de Programa Red de Datos.
4. Correo de reporte: plataformas@udistrital.edu.co

- Consulte el documento *¿Qué es la privacidad de datos?*, de la empresa Kaspersky*.
- Para mayor información sobre términos de seguridad informática, consulte el *Glosario de términos de ciberseguridad*del INCIDE y el *glosario del MinTIC.*

No se pierda nuestros próximos boletines informativos que se publicarán en la página web.

VIGILADO MINEDUCACIÓN - DISEÑO: RED DE DATOS UDNET - CORRECCIÓN DE ESTILO: UNIDAD DE PUBLICACIONES