



Amenazas de seguridad internas: cómo prevenirlas



¿Qué son las amenazas de seguridad internas?

Las amenazas internas en la Universidad Distrital pueden originarse en acciones u omisiones de personas que tienen acceso autorizado a los sistemas, las plataformas o los datos de una organización. Aplica para estudiantes, profesores, personal administrativo, entre otros roles.

Estas situaciones pueden ser intencionales, como el uso indebido de información, o accidentales, como compartir archivos con destinatarios equivocados, utilizar contraseñas inseguras o descargar archivos maliciosos.

¿Cómo pueden afectar a la Universidad Distrital?



Exposición de información:

Divulgación no autorizada de documentos o datos institucionales.



Interrupción de servicios:

Eliminación de archivos o cambios que afecten los servicios tecnológicos.



Compromiso de cuentas:

Uso indebido de credenciales para acceder a sistemas o información.

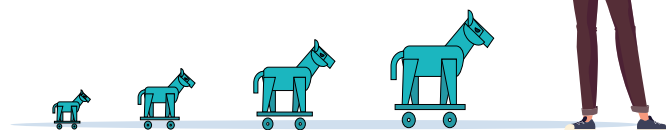


Impacto institucional:

Afectación de las actividades, la confianza y la seguridad de la información de la Universidad.

¿Por qué representan una amenaza?

Las amenazas internas representan un riesgo porque quienes tienen acceso autorizado pueden comprometer información o servicios institucionales mediante acciones indebidas, errores o descuidos. Por ello, es fundamental limitar los accesos y utilizar los recursos tecnológicos de forma responsable.



Señales de alerta



Accesos a sistemas o información no autorizados.



Descargas, copias o transferencias inusuales de información institucionales.



Solicitudes sospechosas de credenciales o permisos.



Uso de cuentas o contraseñas ajenas.



Modificación o divulgación no autorizado de información.

Importante: una señal aislada no demuestra que exista una amenaza. Estas situaciones deben evaluarse según el contexto y reportarse a través de los canales institucionales correspondientes.

Buenas prácticas digitales



No compartas contraseñas ni códigos de verificación. Utiliza los mecanismos de autenticación definidos por la Universidad Distrital.



Utiliza los sistemas y la información de acuerdo con tus funciones y las autorizaciones asignadas.



Revisa destinatarios, permisos y enlaces antes de enviar documentos o habilitar el acceso a archivos institucionales.



Evita aplicaciones, dispositivos o servicios personales no aprobados para almacenar o transferir información institucional.



Bloquea la sesión del computador al alejarte del puesto de trabajo y evita dejar información institucional expuesta.



Informa oportunamente sobre accesos inusuales, pérdida de información, posibles filtraciones o uso indebido de cuentas.



¿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

