UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

BOLETÍN INFORMATIVO

Gestión de los Sistemas de Información y las Telecomunicaciones

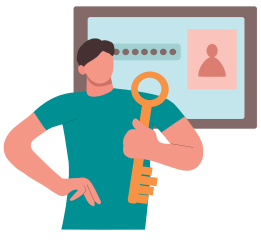
Volumen 2, número 18, septiembre de 2024

¿Qué hacer después de un ataque informático?

Después de un ataque informático, es habitual que la empresa o usuario presten mayor atención, ya que el ciberdelincuente suele recurrir nuevamente sus tácticas de intrusión. Por esta razón, es de vital importancia protegerse para reducir la posibilidad de un nuevo ataque.

Consejos para protegerse después de un ataque informático

01 No use la misma contraseña en los diferentes portales (usuario de dominio, redes sociales, correo electrónico, sistemas de almacenamiento, entre otros). Si el ciberdelincuente logra descubrir alguna de sus credenciales, podrá acceder a las demás cuentas sin problemas.



02 Utilice correctamente sus contraseñas y cámbielas por seguridad periódicamente. Cabe resaltar que son personales e intransferibles; no deje las credenciales a la vista, ni siquiera de personas que considere confiables.

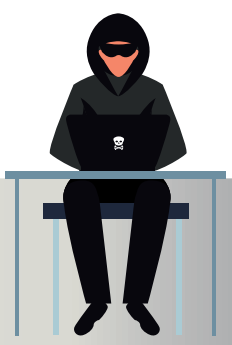
03 Tenga cuidado con los dispositivos extraíbles que conectó antes del ataque, ya que podrían propagar el virus informático a otros dispositivos sin que usted lo note.

04 Use un navegador seguro, mantenga actualizaciones al día y no desactive las opciones de seguridad, como la solicitud de permisos o la ejecución de programas.

05 Mantener el antivirus de su computador personal o el de su oficina activo y actualizado en todo momento. En caso de algún problema en el equipo de su oficina, contacte al personal de soporte.

06 Actualice los sistemas y utilice las últimas versiones, ya que las mismas empresas suelen mejorar la seguridad de sus productos con cada nueva actualización.

07 Habilite autenticación en dos pasos MFA; una medida de seguridad eficaz para proteger sus cuentas y dispositivos.



Si nota que alguno de sus sistemas está funcionando de manera inusual, como la aparición de archivos nuevos o una lentitud inusual, comuníquese de inmediato con el personal de soporte para revisar el equipo.

- Consulte el documento *Buenas practicas tras incidente de seguridad*, 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