SEGURIDAD EN TIEMPOS DE CRISIS

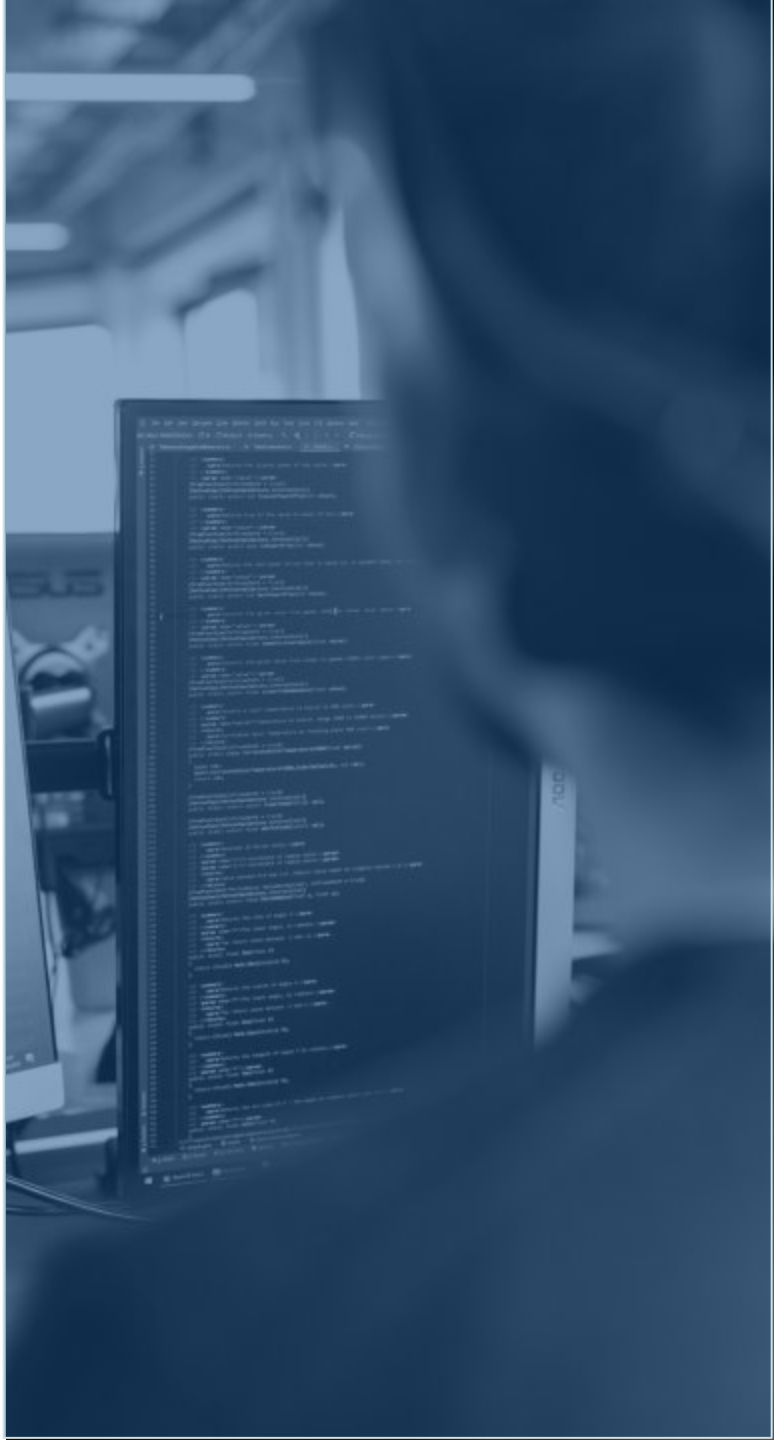
March, 2022

Powered by CYBERREADY

Por qué es importante

La actividad cibernética en torno al conflicto entre Rusia y Ucrania va en aumento y, aunque no estemos directamente involucrados en él, todos nos vemos afectados.

En toda crisis mundial hay una dimensión cibernética, y la creciente cantidad de intentos de phishing mediante mensajes electrónicos maliciosos demuestra que esta crisis no es diferente.



Qué ocurre

1. Ambos lados han lanzado ataques cibernéticos recíprocos, que incluyen programas maliciosos de borrado de datos y sitios web desconectados para impedir su uso legítimo.

2. No siempre se logra contener estos ataques y, a menudo, se infectan dispositivos y sitios web no implicados en el conflicto. Esto también incluye sus dispositivos corporativos o personales.

3. Sus cuentas personales en las redes sociales también corren el riesgo de ser pirateadas para divulgar información falsa o programas maliciosos.

Qué puede hacer para proteger su red doméstica

Instale las actualizaciones más recientes del sistema operativo y de seguridad. Si se encuentran disponibles, en su ordenador o en su teléfono figurará una notificación.

Añada un segundo factor de autenticación a sus cuentas de redes sociales —Facebook, Linkedin, Twitter, etc.— y a sus cuentas de correo electrónico. De ser posible, añada también una cuenta de correo electrónico de respaldo.

Cuente a sus amigos y familiares qué ocurre y anímeles a hacer lo mismo.

Qué puede hacer para proteger nuestra red

Nosotros nos encargamos de la seguridad de la red interna, de modo que no hay nada que deba hacer en el ámbito técnico.

En momentos como estos puede que reciba más ataques de phishing. Desconfíe de mensajes en los que se solicita su ayuda en asuntos técnicos o financieros.

No deje de comprobar la dirección de correo electrónico del remitente. Recuerde que se trata del paso más crucial para detectar un intento de phishing.