SISTEMAS DE ALERTA

El Banco de Desarrollo del Ecuador B.P. se interesa por el bienestar de sus usuarios a efectos de que no sean víctimas de ataques cibernéticos.

Los ataques cibernéticos son cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático.

Con el propósito de precautelar el daño de su ordenador o dispositivo móvil, evitar acceso a información personal e institucional, minimizar el riesgo de extraer contraseñas, fraudes, robo de dinero, etc., por hackers o terceras personas el BDE pone a consideración de los usuarios y público en general las siguientes recomendaciones:

RECOMENDACIONES:

Contar con sitio web con seguros ante ataques informáticos y bancarios, certificados de seguridad con respaldo, filtros de tráfico como Clowdfare (o similares) y evitar planes de hosting compartidos.
Realizar copias de seguridad de sitio web, contenidos, documentos e información regularmente.
Confirmar que el sistema operativo cuente con los últimos parches de seguridad y sitio web, aplicaciones y blog con versiones y plugins siempre actualizados y confiables.
No utilizar software pirata y evitar generar descargas de “Torrents” o procedencia peligrosa.
Usar contraseñas grandes y complejas.
Descargar solo en sitios oficiales.
No abrir ni responder correos electrónicos de dudosa procedencia o remitentes desconocidos, ni dar clic en enlaces adjuntos.
Evitar abrir archivos con extensiones como “archivo.txt.vbs”.
No aceptar enlaces “pop-ups” (ventanas emergentes) sospechosos.
Utilizar herramientas gratuitas como programas comerciales antivirus que ayude a proteger su ordenador o dispositivo electrónico.
Encriptar tus datos mediante configuración avanzada de tu PC, para que solo tú puedas acceder a ellos.
Realizar limpieza periódica de los archivos temporales y de las navegaciones históricas.
No registrar la cuenta de correo institucional en redes sociales o sitios de compras por internet u otro sitio de carácter NO INSTITUCIONAL.
Verificar que su antivirus esté activado y actualizado.
Asegurar el cierre de la sesión al terminar cada actividad planificada.