Reapertura de la oficina

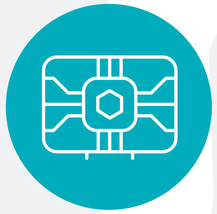
Fundamentos de la ciberseguridad y la protección de datos

01 Seguridad física

Asegúrese de que los controles de seguridad física, la identificación de los empleados y los medios físicos estén actualizados y completamente operativos

02 Privacidad y protección de datos

Busque el consejo del responsable de protección de datos o del responsable de privacidad sobre el impacto de los cambios realizados en los procesos existentes o los nuevos procesos en los que se registran y recopilan datos. Llevar a cabo evaluaciones de impacto en la privacidad (PIA) cuando sea relevante.



03 Gestión de activos

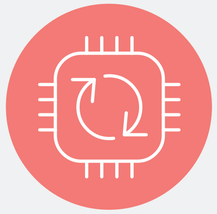
Vuelva a evaluar las políticas de traer su propio dispositivo (BYOD) y asegúrese de que todos los activos no inventariados se registren correctamente.

04 Control de acceso

Garantice credenciales como la autenticación multifactor (MFA) y lque a caducidad y el restablecimiento de la contraseña estén actualizados.

05 Seguridad de la red

El acceso remoto sigue siendo importante durante un regreso paulatino al trabajo, así que mantenga los servicios de red como las redes privadas virtuales (VPN) accesibles y seguros.



06 Seguridad de las operaciones

Las organizaciones deben reevaluar cualquier configuración que hayan realizado durante el período de trabajo desde casa para asegurarse de que siguen siendo las más efectivas.

07 Gestión de vulnerabilidades

La corrección de fallos es un desafío incluso para una organización resiliente a la información. Al regresar a la oficina, las organizaciones deben evaluar su postura y encontrar las correcciones de fallos prioritarias.

08 Continuidad de negocio

Ha llegado el momento de aprender de las actividades recientes, del paradigma del trabajo a distancia, y aplicar los conocimientos adquiridos para mejorar la preparación del plan de continuidad de negocio.

09 Gestión de incidentes

La respuesta a incidentes representa la última línea de defensa en caso de que se materialice un ataque. Asegúrese de que su organización esté preparada para responder a una violación de datos

10 Gobernanza de seguridad

Los registros de riesgos deben reevaluarse dado el panorama de amenazas y el plano de control recientemente reestructurados.

bsi.

Saber más

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

España
+34 91 400 86 209
info.esp@bsigroup.com
bsigroup.com/cyber-es