QUE SEGUROES TU RED?

Utilizar esta**Lista de verificación de preparación para amenazas de 15 puntos**para ayudarle a evaluar la seguridad de la red de su organización. para cada uno de lo siguiente, pregúntese si su organización ha alcanzado el nivel de seguridad deseado. Luego, ingrese el número total de marcas de verificación en la parte inferior para obtener más información sobre la preparación para amenazas de su red.

Marque las casillas para las respuestas SÍ y calcule sus puntos.

Acceso remoto

- ☐ Los empleados y contratistas remotos se conectan a la red corporativa mediante una VPN.
- ☐ Solo los activos de propiedad corporativa pueden conectarse a la VPN.
- ☐ La política de seguridad corporativa, como las políticas antivirus y de parches, se aplican en los puntos finales que se conectan a la VPN.

Conexiones de red

- ☐ Los dispositivos corporativos que se conectan a su red se auditan para verificar el estado del dispositivo y las actualizaciones de los sistemas.
- ☐ Los dispositivos corporativos se conectan a su red inalámbrica mediante un método de conexión que no sea una clave precompartida.
- ☐ Los dispositivos y los usuarios se conectan a su red según las políticas de control de acceso basado en roles (RBAC).
- ☐ Los usuarios y dispositivos no autorizados no pueden acceder a su red a través de una conexión cableada.
- ☐ El acceso se puede controlar dinámicamente si un dispositivo no autenticado se conecta a su red.
- ☐ Se puede restringir el acceso entre dispositivos (tráfico este-oeste) en su red.

Visibilidad

- ☐ La identidad, ubicación y comportamiento de los dispositivos conectados a su red es fácilmente auditable.
- ☐ Sus conjuntos de herramientas de seguridad brindan información sobre los dispositivos conectados que se utilizan para influir en su acceso a su red.

Administración de dispositivos

- ☐ La conexión a dispositivos de red para funciones administrativas se autentica a través de una fuente centralizada.
- ☐ La funcionalidad Multi-Factor Authentication (MFA) está disponible para el acceso administrativo a los dispositivos de red.
- ☐ Es fácil auditar quién se ha conectado a qué dispositivo de red y qué comandos se ejecutaron mientras estaba conectado.
- ☐ El acceso a sus dispositivos de red se puede controlar fácilmente a través de RBAC cuando, por ejemplo, un contratista viene a trabajar en la red.

Tu total: 0

Puntaje:

11- 15	6 - 10	0 - 5
PREPARADO PARA AMENAZA	NECESIDADES MEJORA	VULNERABLE
¡Buen trabajo! El entorno de seguridad de su red cuenta con la mayoría de los controles para mantener seguros los datos de su organización. Contáctenos para saber cómo podemos ayudarlo a mantenerse seguro en un panorama de seguridad cibernética en evolución.	Estás en camino. Desarrollar una hoja de ruta de seguridad de red sólida lleva tiempo. Comuníquese con nosotros para obtener más información sobre lo que Ignite Security puede hacer para ayudarlo a lograrlo.	Su organización está en riesgo. Contáctenos hoy para obtener más información sobre lo que puede hacer ahora mismo para garantizar que su los datos de la organización están protegidos.

SEND MY SCORE

403 252 8550
seguridad@ignitetechnology.com.
www.ignitetechnology.com/seguridad

Sede Corporativa
110, 6825 Calle Ferrocarril SE
Calgary, Ab T2H 2V6

Sucursales
Vancouver, BC | Edmonton, AB | Toronto, ON
Fredericton, NB | Halifax, Nueva Zelanda | San Juan, NL