Lista para comprobar:

CÓMO SABER SI SU RED ESTÁ PROTEGIDA

FORCEPOINT

Si quiere saber el estado en el que está la seguridad en su empresa, esta es la lista que debe tener a la mano. Saque un lápiz y verifique en cada campo cuáles de estos ítems está llevando a cabo.

Señale con una marca de verificación cada vez que la pregunta tenga una respuesta positiva:

1. Lista de verificación de seguridad

Todas las empresas deben tener un plan de seguridad de red escrito (y cuidadosamente preparado) en la compañía. Una política exhaustiva debe cubrir los siguientes temas. Pregúntese:

- [ ] ¿Tiene una política de uso completa que especifique qué tipos de actividades de la red están permitidas y cuáles están prohibidas?
- [ ] ¿Tiene políticas para el manejo del correo electrónico y comunicaciones que ayuden a minimizar los problemas con los emails y archivos adjuntos?
- [ ] ¿Tiene una Política antivirus que ayude a proteger la red contra amenazas como virus, gusanos y caballos de Troya?
- [ ] ¿Tiene una Política de encriptación para proporcionar una orientación sobre el uso de tecnología de cifrado para proteger los datos de red?

- [ ] ¿Tiene una Política de acceso remoto para ayudar a los empleados a acceder de forma segura a la red cuando trabajan fuera de la oficina?

- [ ] ¿Tiene una Política de identidad que ayude a proteger la red de usuarios no autorizados?

- [ ] ¿Tiene una Política de contraseñas, para ayudar a los empleados a seleccionar contraseñas seguras y protegerlas?

2. Inventario de sus tecnologías de seguridad actuales

¿Cuenta con alguno de los siguientes sistemas?

- [ ] Firewall, para mantener a los usuarios no autorizados fuera de su red.

- [ ] Red privada virtual (VPN), para brindar a los empleados, clientes y socios un acceso seguro a su red.

- [ ] Red inalámbrica segura, para proporcionar acceso de red seguro a los visitantes y empleados en el camino.

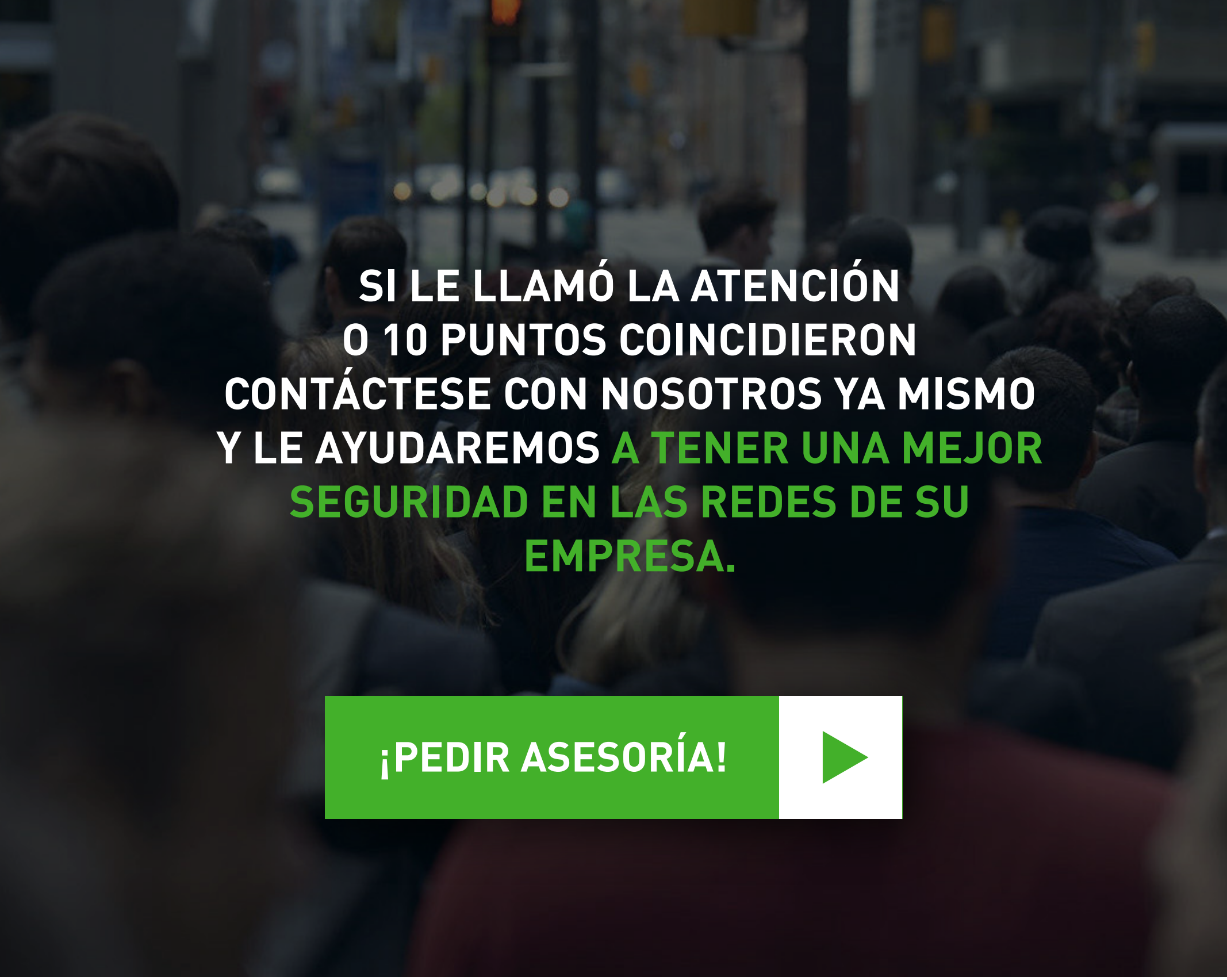
- [ ] Validación de cumplimiento para asegurarse de que cualquier dispositivo que acceda a la red cumpla con sus requisitos de seguridad.
- [ ] Prevención de intrusos, para detectar y detener amenazas antes de que dañen su red.
- [ ] Gestión de identidad para darle control sobre quién y qué puede acceder a la red.
- [ ] Seguridad de contenido para proteger su red de virus, spam, spyware y otros ataques.

Si en muchos de estos campos usted no señaló con una marca de verificación es probable que necesite ayuda con seguridad para la nube, seguridad de redes, protección de datos y contra amenazas internas. En Forcepoint estamos listos para ayudarle. **¡Contáctenos!**

Además de este checklist, lo invitamos a hacerse estas preguntas sobre sus activos digitales más importantes y quiénes los usan en su empresa. ¿Realmente está asegurado?

- ✔ **¿Cuáles son exactamente los activos digitales de su empresa (como propiedad intelectual y registros de clientes)?**

- ¿Dónde están esos activos?
- ¿Quién tiene acceso a estos activos y por qué? ¿Todos los empleados pueden acceder a los mismos activos?
- ¿Cuál es el impacto financiero potencial de una interrupción de la red debido a una violación de seguridad?
- ¿Podría una brecha de seguridad interrumpir su cadena de suministro?
- ¿Tiene funciones de comercio electrónico en su sitio?
- ¿Cuánto tiempo podría estar el sitio antes de perder dinero?
- ¿Está asegurado contra ataques de Internet o contra el mal uso de los datos de sus clientes? ¿Es este seguro adecuado?
- ¿Tiene capacidades de respaldo y recuperación para restaurar la información si es necesario después de una violación de seguridad?



SI LE LLAMÓ LA ATENCIÓN
O 10 PUNTOS COINCIDIERON
CONTÁCTESE CON NOSOTROS YA MISMO
Y LE AYUDAREMOS A TENER UNA MEJOR
SEGURIDAD EN LAS REDES DE SU
EMPRESA.

¡PEDIR ASESORÍA!

FORCEPOINT