cisco SECURE Partner

CINCO SUGERENCIAS PARA PROTEGER SU FUERZA DE TRABAJO HÍBRIDA

A medida que el mundo hace la transición a una fuerza laboral híbrida más permanente, la flexibilidad ofrece nuevos beneficios y desafíos para las empresas y los trabajadores. Ya sea que su equipo trabaje en la oficina, de forma remota o una combinación de ambas, no necesita sacrificar su seguridad para obtener mayor flexibilidad. Aquí hay una lista de cinco consejos sencillos para mantener la cultura híbrida de su fuerza laboral y, al mismo tiempo, proteger a sus empleados y los activos de su empresa.

1

Capacite a sus empleados para adoptar prácticas seguras de trabajo

Los empleados esperan que la tecnología los siga a cualquier lugar, pero tener ubicaciones flexibles los expone (y a su organización también) a nuevas amenazas. Por lo tanto, los equipos de TI y de seguridad deben garantizar que la experiencia híbrida sea segura en todas las terminales mediante la capacitación a los usuarios acerca de prácticas seguras y posibles riesgos.

2

Verifique la identidad de las personas

La autenticación de múltiples factores (MFA) es una sencilla capa inicial de seguridad que toda empresa debe tener antes de otorgar acceso a sus recursos empresariales. Piense en la autenticación MFA como un amigo cercano a quien conoce bien (su usuario y clave) y como un artículo cotidiano (su teléfono) que verifica su identidad y garantiza su seguridad.

3

Habilite el acceso seguro desde cualquier lugar

La VPN proporciona un túnel seguro entre los usuarios y las aplicaciones para que los trabajadores mantengan su productividad y permanezcan conectados sobre la marcha o trabajando desde casa. Garantiza que solo los usuarios autorizados accedan a la red con un nivel de seguridad óptimo sin entorpecer la experiencia del usuario.

4

Defiéndase contra amenazas de seguridad en cualquier punto de entrada

La mayoría de las filtraciones de seguridad atacan el punto final de los usuarios, por lo que se requiere implementar una primera línea de defensa en la capa de DNS y una solución final para proteger contra las amenazas que logren filtrarse. La primera capa bloquea los dominios asociados con conductas maliciosas antes de que accedan a la red o contiene al malware si ya está dentro de esta. Y la última capa protege contra amenazas más avanzadas.

5

Unifique su seguridad en una plataforma simple e integrada

No sacrifique su seguridad con productos inconexos y experiencias de usuario dispares. Simplifique y optimice su seguridad con SecureX, una plataforma perfectamente integrada que conecta a la perfección sus productos Cisco Secure con su infraestructura.

Mantenga sus datos seguros en dondequiera que sus empleados trabajen con Cisco Secure Hybrid Work, una solución simple y unificada para asegurar la seguridad en todas partes y potenciar el trabajo desde cualquier lugar.
Más información en: cisco.com/go/securehybridwork.

boyra
comunica tus sueños

TELEFONOS: 57 6019156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM