


Aprendiendo del COVID-19: Planificación de la Continuidad y Seguridad

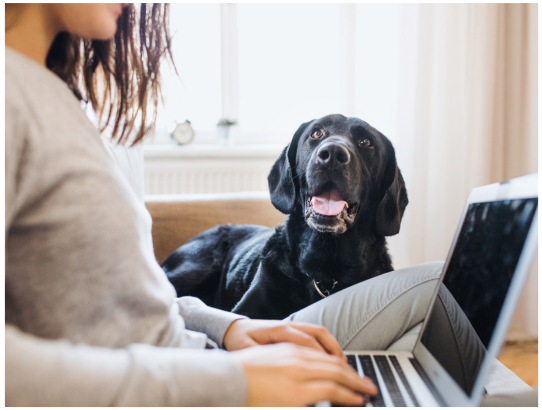
WatchGuard®

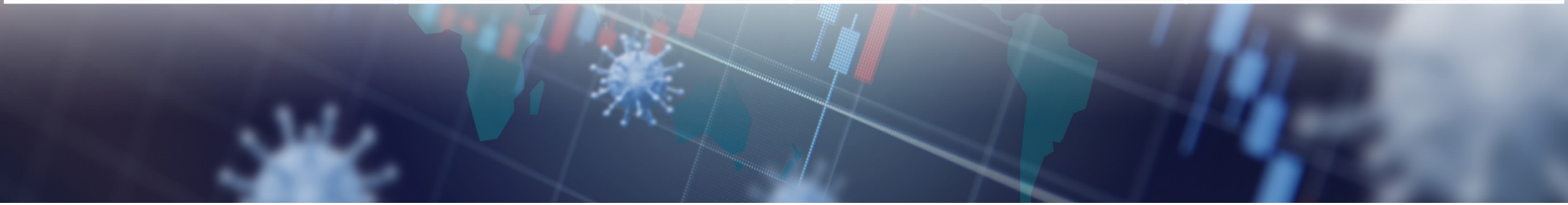
Índice

INTRODUCCIÓN

A medida que la sociedad se enfrenta a una muy seria pandemia, el nuevo coronavirus (COVID-19) afecta a casi todo el mundo. Las escuelas están cerradas, hay restricciones para viajar, los eventos han sido cancelados y las oficinas están vacías; todo esto con el objetivo de detener la propagación del COVID-19. El Centro de Control de Enfermedades ha llegado a sugerir a los empleadores que establezcan políticas que permitan a sus empleados trabajar de manera remota a fin de promover el distanciamiento social. Sin perder el tiempo, las empresas han tomado rápidamente las acciones para responder a la amenaza y, como resultado, hoy hay más personas trabajando desde sus hogares que en cualquier otro momento de la historia moderna. Y para darles una simple idea de cuán problemático puede ser esto, según un estudio, el personal remoto de Norteamérica ha crecido un 159% entre el 2005 y el 2017. Vale decir que en la actualidad, debido al brote del coronavirus, estamos frente a números mucho más grandes.

La respuesta al coronavirus no tiene precedentes y este experimento del "trabajo desde casa" lleva a muchas empresas a un territorio decididamente desconocido. En este libro electrónico detallaremos las estrategias para mantener la continuidad del negocio durante el brote del coronavirus.





ANÁLISIS DEL PANORAMA DEL COVID-19:
DESAFÍOS ACTUALES PARA LA CONTINUIDAD DEL NEGOCIO

Nos enfrentamos a riesgos de seguridad cibernética todos los días. Sin embargo, uno de los desafíos de facilitar personal móvil es que las probabilidades de sufrir ataques cibernéticos pueden aumentar significativamente. Sin el beneficio de sus protecciones de red fundamentales, un usuario en movimiento puede infectarse sin saberlo e, incluso, infectar a un entorno más amplio al volver a conectarse a su red.

Los hackers se aprovechan de los temores al coronavirus

Se sabe que los hackers tomarán ventaja de cualquier noticia importante o evento mundial para lanzar sus ataques. En un momento de temor intensificado, las cuentas de correo electrónico y redes sociales de sus empleados están inundadas de nuevos reportes, comentarios, videos y enlaces sobre el virus. Lamentablemente, los criminales cibernéticos se aprovechan de los temores para suplantar la identidad de sus usuarios, atacar sus sistemas o diseminar malware.

Estos son algunos ejemplos de cómo obtienen ventajas del coronavirus:

- **Suplantación de la identidad de la Organización Mundial de la Salud** (OMS). La OMS ha reportado mensajes sospechosos de suplantación de identidad en los que se da información crítica de salud en su nombre. En ellos se solicitaba a las víctimas que hicieran clic en un enlace, descargaran un archivo o proporcionaran información confidencial.
- **Diseminación de Malware.** Un grupo de hackers ha aprovechado la pandemia del coronavirus para infectar a víctimas de Mongolia con un malware ya conocido, en una campaña recientemente descubierta que se conoce con el nombre de "Vicious Panda."
- **Diseminación del Troyano Emotet a Través del Correo No Deseado**. Los hackers utilizan noticias aparentemente útiles sobre cómo impedir la diseminación de usuarios afectados por el coronavirus en Japón como parte de una campaña de correos no deseados diseñada para diseminar el troyano Emotet. El Emotet puede secuestrar cuentas de correo electrónico y suplantar mensajes para infiltrarse en un entorno.
- **Aplicación Falsa de Rastreo de Virus Que Disemina Ransomware.** Se trata de una aplicación que simula ser un rastreador de mapas del brote de coronavirus cuando en realidad es un ransomware que bloquea su teléfono. La aplicación, "COVID19 Tracker", infecta su dispositivo y exige USD 100 en Bitcoin dentro de las 48 horas.

Novatos Fuera de la Red

El COVID-19 está impulsando políticas agresivas de "trabajo desde casa" y, como consecuencia, las empresas están cerrando sus oficinas y enviando a sus empleados a trabajar desde casa tiempo completo casi de la noche a la mañana. A pesar de que la flexibilidad del lugar de trabajo es ahora la norma para muchas empresas, en promedio solo cerca del 30% del personal trabaja desde su casa en un horario establecido. Muchas empresas han hecho un gran esfuerzo para brindar los recursos necesarios para que sus empleados sigan estando protegidos al trabajar desde casa. Los han provisto rápidamente de computadoras portátiles o los han enviado a casa con computadoras de escritorio que no se suponía en absoluto que quedaran fuera de la red segura. Estos dispositivos no solo necesitan seguridad ahora que están fuera de la red, sino que además es importante que nos aseguremos de que no permitan el ingreso de malware y otras amenazas cuando se vuelvan a conectar a la red, ya sea a través de VPN o al volver a la oficina.

VPN Sobrecargadas

Debido a que se ha enviado masivamente a los empleados a trabajar desde sus casas por el coronavirus, el uso de las VPN ha aumentado vertiginosamente y los investigadores han observado un incremento del 50% en el tráfico de red en solo una semana. Solo en Estados Unidos se espera que aumente el uso de VPN un 150% en un mes. La migración repentina de los usuarios de la oficina al hogar ha hecho que muchas empresas deban ingeniárselas para ofrecer licencias de VPN a sus empleados. El riesgo es que sin conectividad VPN, los usuarios no tendrán acceso a los recursos que necesitan o utilizarán conexiones inseguras para acceder a ellos.

Caos en el Ancho de Banda

Los empleados no son los únicos que están en sus hogares. Con las escuelas cerradas, muchos de sus colegas tendrán a sus hijos en casa accediendo a educación remota, jugando o simplemente navegando en la web. Estos dos grupos consumirán a toda velocidad el ancho de banda, en especial cuando utilicen aplicaciones que requieren muchos recursos como las videoconferencias. Los lugares donde el virus ha impactado con mayor fuerza han tenido un aumento de más del 90% en el uso de Internet. Como respuesta, muchos proveedores de servicios de Internet (ISP) ofrecen a sus clientes conexiones más rápidas y con un ancho de banda superior o eliminan el límite de datos para evitar que se exceda.

El uso de las VPN ha aumentado vertiginosamente, **con un incremento del 50% en el tráfico de red en solo una semana**. Solo en Estados Unidos se espera que **aumente el uso de VPN un 150% en un mes.**

OCHO CONSEJOS PARA LOS LÍDERES DE TI SOBRE EL USO DE LA SEGURIDAD COMO HERRAMIENTA FACILITADORA DE PRODUCTIVIDAD Y ACCESO

1. EVALÚE LAS CAPACIDADES DE TRABAJO REMOTO QUE TIENE SU EMPRESA.

A pesar de que el 92% de las empresas ofrece trabajo remoto, no se ha ofrecido esa opción a todos los empleados de manera equitativa. Para muchas empresas, este paso al trabajo remoto sucedió prácticamente de la noche a la mañana y les dio muy poco tiempo para una planificación adecuada. Ahora es el momento de auditar y evaluar el nuevo acceso a la red que requiere su empresa, y tener en cuenta las consecuencias que eso puede tener en la seguridad. Los proveedores de servicios de seguridad administrada (MSSP) son expertos en evaluación de seguridad y pueden ayudar a las medianas empresas a lograr estar a la altura rápidamente y brindar a sus usuarios lo que necesitan.

Lo más probable es que los usuarios itinerantes de la red, que siempre están en movimiento, tengan los recursos necesarios para este largo recorrido. Para aquellos que no han trabajado tanto desde casa, es útil hacer un inventario de todos los datos y aplicaciones a las que acceden de manera regular. Con esta información, puede definir a qué es necesario acceder, quién necesita ese acceso y cuál es la mejor manera de proporcionarlo. Trabaje con los jefes de departamento para comprender las necesidades específicas de su equipo y asegúrese de que los miembros del equipo estén preparados para el éxito.

Esta es una lista de comprobación de lo que debe tener en cuenta:

- ¿El empleado tiene un dispositivo autorizado o debe adquirir más teléfonos o computadoras portátiles?
- ¿Dispone de suficientes licencias de VPN para otorgarlas a quienes las requieran o necesita adquirir más?
- ¿El empleado tiene un acceso adecuado a Internet para realizar su trabajo?
- ¿Qué sistemas requiere el empleado para realizar su trabajo?
- ¿El empleado requiere acceso seguro a sistemas y datos confidenciales?
- ¿Qué aplicaciones en la nube utiliza el empleado de manera habitual?
- ¿El empleado tiene configurada la autenticación multifactor?

2. ESTABLEZCA LAS EXPECTATIVAS PARA EL TRABAJO REMOTO Y COMUNÍQUELAS

Debido a que es probable que muchos de sus empleados estén trabajando desde sus casas por primera vez, es un excelente momento para contactar a su equipo y explicarle las políticas de su empresa respecto al "trabajo desde casa" para establecer las expectativas en relación a los empleados que trabajan de manera remota. Alrededor del 24% de las empresas llevan más de un año sin actualizar sus políticas de "trabajo desde casa", de modo que esta es una oportunidad para hacerlo. Un simple correo electrónico, o una llamada en conferencia con su equipo, puede ser muy útil.

Estos son algunos de los temas que es recomendable abordar:

- **Disponibilidad:** ¿Cuál es el horario de trabajo que espera que cumpla su equipo? ¿En qué horario estará usted disponible?
- **Capacidad de Respuesta:** ¿Se espera que los trabajadores remotos respondan de manera inmediata? De ser así, ¿cómo se comunicará esa expectativa? Por ejemplo, ¿las solicitudes realmente urgentes se realizarán solo por teléfono?
- **Plataformas:** Recuerde a sus empleados qué herramientas y plataformas deben utilizar, incluidas las plataformas de almacenamiento en la nube, las herramientas de comunicación/videoconferencia, las herramientas de administración de proyectos, etc. Fomente en su equipo el uso de plataformas autorizadas solamente.
- **Dispositivos:** Si su equipo tiene dispositivos otorgados por la empresa, recuérdeles las políticas que ha establecido con respecto al uso de esos dispositivos. Si están utilizando sus propios dispositivos personales para trabajar, es un buen momento para ofrecerles orientación con respecto a qué dispositivos es apropiado usar y de qué manera deben realizar negocios en esos dispositivos.
- **Notificación de Incidentes:** ¿A quién debe recurrir un empleado si cree que la información de la empresa podría verse comprometida? ¿A quién debe dirigirse para informar sobre la vulneración de datos y qué pasos debe tomar para minimizar los efectos secundarios?

3. PROMUEVA LA CULTURA DE LA SEGURIDAD CIBERNÉTICA

La mayoría de los líderes empresariales comprenden que la cultura de un lugar de trabajo es una parte importante del éxito o del fracaso. También deben comprender que la misma dinámica existe en la seguridad cibernética. Debido a que sus empleados están bajo amenaza de ataques dirigidos, y en algunos casos los atacantes se hacen pasar por miembros de su equipo, la cultura corporativa con frecuencia termina siendo un factor determinante que consigue interceptar el ataque o infectar a toda su red.

Los hackers utilizan técnicas para manipular a sus usuarios e influir en ellos para que actúen como ellos quieren, usando como arma la autoridad y la urgencia. Como líder, usted debe estimular el uso de canales de comunicación abiertos, de forma tal que cuando un empleado, incluso los de menor jerarquía de la organización, vea algo que considere una amenaza, sienta la tranquilidad de que su preocupación será tenida en cuenta.

Consejos para promover la cultura de seguridad cibernética:

- **Compartir historias.** ¿Un empleado abrió un correo electrónico de suplantación de identidad o ha entrado ransomware en su computadora portátil? Compartir la historia con la empresa puede ayudar a que los empleados comprendan que las amenazas son reales y que otras personas eviten ataques similares. Compartir noticias sobre ataques contra empresas similares también puede ayudar.
- **Premiar un comportamiento.** Cuando un empleado informa sobre un posible ataque, podría estar ahorrándole a su empresa un enorme problema. Entonces, ¿por qué no premiar su comportamiento? Incentivar a sus empleados a que informen sobre actividades sospechosas puede contribuir a generar concientización y lograr que otros se involucren.
- **Ser amable.** Seamos honestos, en las empresas las habilidades tecnológicas varían de persona a persona. No es realista pensar que sus empleados van a poder evitar todas las amenazas y seguir todas las políticas. Las personas cometen errores. Por eso es tan importante brindar apoyo.

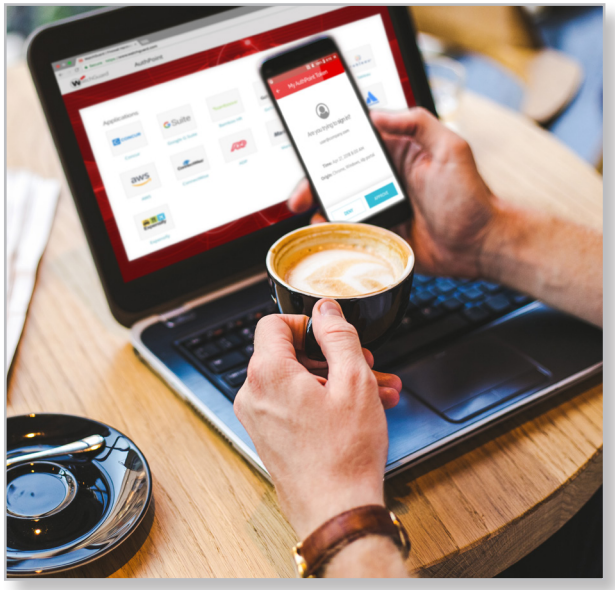
4. IMPLEMENTE LA AUTENTICACIÓN MULTIFACTOR

Mientras las empresas luchan por conseguir que la mayor parte de su personal pueda trabajar de manera remota, garantizar el acceso a las herramientas internas es un enorme desafío. Al mismo tiempo, los hackers tienen cada vez más interés en las credenciales, y tienen la mira puesta en la información de las cuentas de sus usuarios. Por este motivo, recomendamos implementar la autenticación multifactor (MFA) para todos los usuarios, de forma tal que pasen por una autenticación completa cada vez que se conecten a su red.

La autenticación multifactor le permite, además, proteger el acceso a aplicaciones y entornos en la nube a los que los trabajadores remotos podrían acceder directamente desde Internet, lo cual ofrece una capa adicional de protección en un momento en que las empresas son muy vulnerables.

Lo que debe buscar en una solución de MFA:

- **Disponibilidad en la nube.** A diferencia de las MFA que requiere un token de hardware, las soluciones basadas en la nube permiten al usuario descargar una aplicación en su teléfono y empezar a utilizarla de inmediato.
- **Cobertura de aplicaciones.** La solución debe integrarse para proteger a todas las aplicaciones críticas que sus empleados necesitan.
- **Simplicidad.** La solución debe ser intuitiva para usuarios con diversos niveles de capacidad técnica.
- **Varios métodos de autenticación.** La existencia de varias opciones de autenticación en línea y fuera de línea garantiza que los usuarios autorizados puedan acceder a lo que necesitan, cuando lo necesitan.
- **Soporte de múltiples tokens.** Hoy, es común que se ofrezca MFA en los sitios de redes sociales, los bancos, los minoristas y más. Busque una solución que le permita consolidar tokens en una simple aplicación de MFA para simplificar el acceso de sus usuarios.



5. AMPLÍE EL ACCESO DE VPN A USUARIOS PRIORITARIOS

Una conectividad segura a las oficinas centrales corporativas y a las aplicaciones críticas es fundamental si quiere que sus empleados mantengan la productividad al trabajar de manera remota. Las redes privadas virtuales (VPN) agregan una capa de seguridad a las redes privadas y públicas, lo que permite a las personas y a las organizaciones enviar y recibir datos de manera segura por Internet.

Por lo general, los usuarios requerirán uno de los siguientes tipos de VPN:

1. **VPN basada en cliente.** Al operar en el nivel de red, la VPN basada en cliente ofrece a los usuarios acceso a toda la red.
2. **VPN sin clientes.** Las VPN sin clientes, que usualmente utilizan solo un explorador, conectan a los usuarios a aplicaciones y servicios específicos.

En general, las empresas solo ofrecen VPN a un grupo limitado de empleados remotos y que viajan con frecuencia, y no a todo el personal. A medida que el uso de la VPN aumenta, tenga en cuenta estos consejos para administrar su uso y evitar problemas:

- **Establezca el uso prioritario de la VPN para usuarios de alto riesgo**. Algunos empleados requerirán mayor acceso que otros y habrá algunos que no necesiten acceso a la VPN. El hecho de comprender quién necesita acceso a qué, y otorgar conectividad de VPN basada en prioridades ayudará a impedir la sobrecarga de la red.
- **Utilice un firewall en la nube para satisfacer la demanda.** El aumento de demanda de servicios de VPN no significa que tenga que liberar espacio en la sala de servidores. Los firewalls hospedados en la nube pueden ayudar a equilibrar la carga del tráfico de VPN destinado a su oficina central y adaptarse para proporcionar las conexiones que su empresa necesita.
- **Exija una MFA.** Sin MFA, un solo conjunto de credenciales de VPN podría darle a un atacante acceso total a su red. Los usuarios que utilizan VPN para conectarse deben pasar por una autenticación completa por medio de dos factores como mínimo.
- **Facilite un firewall de escritorio.** Un firewall de escritorio implementado por un usuario que está trabajando desde casa puede ofrecer protección de UTM completa sin sobrecargar la VPN corporativa.

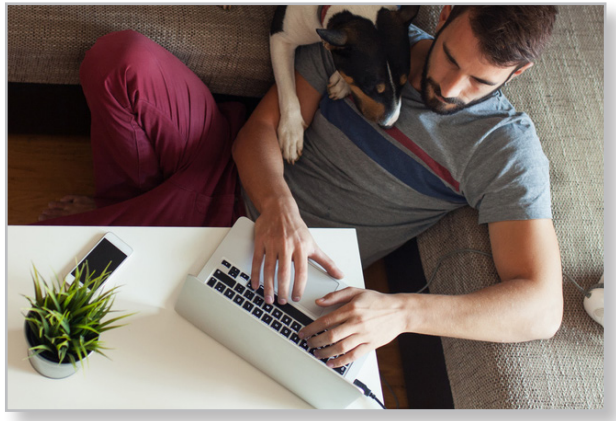
6. MANTENGA A LOS USUARIOS PROTEGIDOS CONTRA CLICS RIESGOSOS CON FILTRADO DE DNS

Proteger a los usuarios cuando navegan por Internet es más difícil cuando se conectan fuera de su red. Con los empleados encerrados en casa, lo más probable es que las computadoras portátiles de la empresa se utilicen en gran medida para navegación personal de la web y para ver el correo electrónico. El filtrado de DNS basado en la nube permite bloquear conexiones y limitar el acceso a áreas riesgosas de Internet. Es posible evitar hacer clic en enlaces maliciosos o intentar conectarse a dominios relacionados con la suplantación de identidad y el malware, sin tener que usar una VPN.

Puntos que debe considerar sobre una solución de filtrado de DNS:

- **Productividad y aplicación de políticas.** Debido a que hay más empleados que trabajan fuera de la oficina, quizás debería restringir el acceso de los usuarios a cierto tipo de contenido, como las redes sociales y sitios para adultos, para que esto no afecte la productividad. Busque controles granulares, como la capacidad de bloquear usuarios y grupos, y establezca horarios de aplicación de las políticas.

- **Apoyo a iniciativas para el entrenamiento de seguridad.** A esta altura, la mayoría de las empresas ofrece alguna forma de entrenamiento de seguridad cibernética a sus empleados y, debido a que están migrando de las instalaciones, reforzar ese entrenamiento es más importante que nunca. Algunas soluciones de filtrado de DNS no solo bloquean las conexiones inseguras, sino que ofrecen al usuario un repaso sobre cómo identificar amenazas similares en el futuro.



7. MANTENGA LOS ENDPOINTS LIBRES DE MALWARE

Como resultado del coronavirus, las amenazas de malware y ransomware han aumentado significativamente. Además, el riesgo de infección nunca ha sido más alto debido a que, al trabajar desde sus casas, los usuarios ya no cuentan con los beneficios de la protección de un firewall. Si bien las soluciones de antivirus de endpoints detectan muchas de las amenazas, no tienen poder alguno frente al malware evasivo de día cero con el que nos enfrentamos muy a menudo. Las soluciones de detección y respuesta de endpoints (EDR) no solo pueden detectar estas amenazas avanzadas, sino que también pueden eliminarlas y hacer que el dispositivo infectado vuelva a funcionar con normalidad, todo de manera remota.

Funcionalidades esenciales de una solución de EDR:

- **Métodos de detección.** Para detectar malware avanzado se requiere de técnicas avanzadas. Busque soluciones que combinen varios métodos de detección, por ejemplo, de comportamiento, heurísticos y de sandbox.

- **Automatización e IA.** Una respuesta rápida a las amenazas puede evitar un gran problema. La automatización de la detección y la respuesta puede hacer que esto suceda de manera casi instantánea.

- **Aislamiento de hosts.** Cuando se detecta una amenaza, se debe eliminar la conectividad del host infectado con otras partes de la red para impedir que se disemine la infección.

8. Conserve el control de la red Wi-Fi

El trabajo remoto puede generar preocupaciones de seguridad relacionadas con Wi-Fi también. Para trabajadores remotos ubicados en zonas residenciales densamente pobladas, como apartamentos o condominios, todos los dispositivos Wi-Fi, entre los que se incluyen timbres, consolas de juegos y dispositivos IoT, pueden convertirse en una puerta de entrada para vecinos maliciosos que buscan entrar sin permiso. Los vecinos maliciosos podrían aprovechar el hecho de que sus edificios están colmados de trabajadores remotos, con casi el 50% del tráfico de IP ocupado por Wi-Fi.

Consideraciones de Wi-Fi para el trabajo remoto:

- **Considere la posibilidad de distribuir puntos de acceso certificados de Entorno Inalámbrico Confiable**, como el AP225W de WatchGuard, para ofrecer a su departamento de TI visibilidad completa del cliente y del rendimiento de la red, con el objetivo de ofrecer un mejor soporte al personal remoto.
- **Configure previamente los puntos de acceso** para que los usuarios puedan implementarlos con facilidad en casa.

En zonas residenciales densamente pobladas, como apartamentos, la red Wi-Fi ocupa casi **el 50% de todo el tráfico de IP**.

POR QUÉ ES IMPORTANTE QUE LOS NEGOCIOS ESTÉN PREPARADOS EN MATERIA DE SEGURIDAD DE TI

En pocas palabras, hay cosas que no se pueden predecir. Los líderes empresariales saben que habrá dificultades y eventos imprevistos en el camino. Entonces, ¿qué puede hacer para proteger el futuro de su empresa? Un plan de preparación no es garantía de perfección, pero puede darle herramientas para enfrentar de manera segura los desafíos y brindarle los recursos necesarios para garantizar la continuidad operativa.

Hoy se trata del brote del coronavirus, pero podría ser cualquier otra cosa y no solo catástrofes. Un importante evento como La Copa del Mundo que altera la manera en que funciona normalmente una ciudad o, incluso, un error humano puede colocar a su empresa en modo de preparación crítica. Cualquier situación que lo obligue a adaptarse rápidamente a cambios inesperados es la prueba irrefutable de la importancia de comprender realmente cómo es su organización y qué necesita.

¿Por qué? Porque les muestra a sus empleados, a sus clientes y a las partes interesadas que su empresa puede salir adelante incluso durante eventos sin precedentes. Sí, esto es grandioso para su marca, pero lo más importante es que crea un gran sentido de confianza en su comunidad. Además, tendrá una historia increíblemente valiosa por muchos años.

¿Por qué? Porque les muestra a sus empleados, a sus clientes y a las partes interesadas que su empresa puede prosperar incluso durante eventos sin precedentes.

LISTA DE COMPROBACIÓN DE CONTINUIDAD DEL NEGOCIO

Evaluación de capacidades de trabajo remoto de su empresa

¿Mi Empresa Está Preparada?	Sí	No	Acción
¿Ha actualizado su política de "trabajo desde casa" en los últimos 12 meses?			
¿Ha comunicado la política y las expectativas a todos los empleados que trabajan ahora desde casa?			
¿Necesita adquirir más teléfonos/computadoras portátiles para garantizar que todos sus empleados tengan un dispositivo autorizado?			
¿Dispone de suficientes licencias de VPN para ofrecerlas según sea necesario?			
¿El empleado tiene un acceso adecuado a Internet para realizar su trabajo?			
¿Ha determinado si los empleados remotos tienen acceso a los sistemas o a las plataformas requeridas para realizar su trabajo de manera correcta? *Es decir, aplicaciones en la nube.*			
¿Su empresa puede ofrecer medidas seguras para evitar riesgos de ataques cibernéticos al trabajar de manera remota? Es *decir, Wi-Fi protegido, conexión de VPN y autenticación multifactor.*			
¿Necesita realizar ajustes a su presupuesto de TI para proporcionar los recursos necesarios?			
¿Necesita ofrecer entrenamiento de seguridad para el trabajo remoto a su personal?			

SERVICIOS GRATUITOS PARA AYUDAR A LAS PEQUEÑAS Y MEDIANAS EMPRESAS DURANTE LOS SUCESOS ACTUALES SIN PRECEDENTES

Por un tiempo limitado, WatchGuard ofrece servicios gratuitos o con descuento para ayudar a las empresas a proteger al personal remoto. Visite nuestra **página de Recursos para Trabajadores Remotos** para obtener información sobre ventas especiales de WatchGuard Passport, un paquete de servicios de seguridad centrados en el usuario diseñado para bloquear los intentos de suplantación de identidad, aplicar las políticas de exploración de web y autenticar a las personas en todas partes del mundo.

Obtenga más información

Para conocer más detalles, comuníquese con un revendedor autorizado de WatchGuard o visite **https://www.watchguard.com.**

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Casi 10.000 revendedores de seguridad y proveedores de servicios confían en los productos y los servicios premiados de la empresa para proteger a más de 80.000 clientes. La misión de WatchGuard es lograr que empresas de todos los tipos y tamaños accedan de manera sencilla a una seguridad de calidad empresarial. Por ello, WatchGuard es una solución ideal para empresas de mercado medio y para empresas distribuidas. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica. Para obtener más información, visite WatchGuard.com.

WatchGuard

Ventas en Norteamérica: 1.800.734.9905 • Ventas internacionales: 1.206.613.0895 • Sitio web: www.watchguard.com