Ciberseguridad: lecciones aprendidas para el funcionamiento del trabajo remoto

kaspersky PREPARADOS PARA EL FUTURO

Las opciones de trabajo flexible y remoto siempre fueron populares entre los empleados. Sin embargo, cuando la pandemia mundial interrumpió las operaciones, prácticamente todas las empresas se vieron en la obligación de abrir sus redes y sistemas para la operación remota.

Un informe indica que un 61 % de las empresas implementó el trabajo remoto para todos sus empleados durante 2021[1]. Las empresas también buscan fomentar esta tendencia: un 24 % tiene la intención de utilizar el trabajo remoto en el futuro[2].

Pero muchas empresas se apresuraron en la implementación del trabajo remoto. La prioridad era mantener cierto nivel de productividad; prácticamente cualquier otra consideración se dejaba de lado para favorecer la velocidad.

Si este fuera el caso de su empresa, ¿puede asegurar que sus disposiciones de trabajo remoto son seguras?

El 61 % de las empresas implementó el trabajo remoto para todos sus empleados en 2021

El 90 % de los profesionales de TI cree que los trabajadores remotos presentan un riesgo de seguridad y un 54 % cree que representan un mayor peligro que sus contrapartes in situ[3]. Claramente, se reconoce que el trabajo remoto puede involucrar grandes riesgos, pero, al mismo tiempo, un 26 % de las empresas informa que no tienen la seguridad suficiente para secundar la fuerza de trabajo remota de forma adecuada[4].

Lo cierto es que, a medida que el mandato de cuarentena entraba en vigor, las empresas se vieron obligadas a implementar disposiciones de trabajo remoto lo más rápido posible. Incluso cuando había sistemas de trabajo remoto en funcionamiento, la mayoría no era capaz de implementarlos de manera apropiada a gran escala.

En muchos casos, esto llevó a una explosión en el uso de la TI invisible, ya que los empleados se apresuraban a fin de encontrar herramientas que fueran lo "suficientemente buenas" para colaborar y compartir datos. La seguridad y el cifrado no se presentaron de forma destacada en muchas de estas elecciones, lo que llevó a la selección de aplicaciones inseguras e inapropiadas[5]. Estas malas elecciones aumentaron de gran manera el riesgo de que se perdieran, robaran o filtraran los datos, especialmente porque no tenían mecanismos de control centralizado que le permitieran al equipo de seguridad de TI monitorear los usos y las vulneraciones.

Debido a que el trabajo remoto se consolidó, las empresas están comenzando a ponerse al día. En los últimos 18 meses, tuvieron el tiempo de evaluar las herramientas y elegir las que protegen de mejor manera los intereses de la organización. Sin embargo, estas disposiciones de trabajo remoto siguen presentando una deficiencia inherente a la forma en la que se elaboraron en sus comienzos.

Esta guía lo ayudará a comprender algunos de los riesgos que enfrenta en términos de endpoints, infraestructura y redes. Además, proporcionará un plan útil para mejorar su postura de seguridad a medida que el perímetro de red se deteriora y se utilizan más dispositivos desconocidos no confiables para acceder a los recursos corporativos.

Sección 1: ¿Sus endpoints están en orden?

Los dispositivos que utilizan los trabajadores son un pilar fundamental en la estrategia del trabajo remoto. Muchos administradores de TI consideran que este es el problema más difícil de resolver, ya que los empleados suelen utilizar los dispositivos personales para trabajar. Esto solo hace que la administración escalable sea aún más difícil.

Un 40 % de los administradores de TI afirma tener dificultades para conseguir el equipamiento adecuado para sus trabajadores remotos[6], motivo por el cual un 61 % de los trabajadores remotos tuvo que abastecerse por sí mismo[7]. En estos casos, un 27 % tuvo problemas con la logística para instalar agentes de administración en sus dispositivos[8]. Sin embargo, debe haber cierto grado de control de endpoints para proteger los recursos corporativos.

Entre las preguntas que debe abordar, están las siguientes:

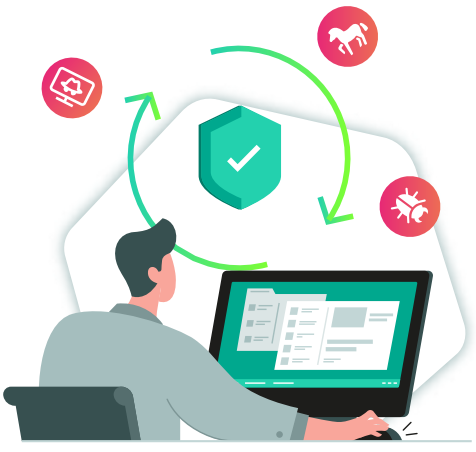
- **¿Estamos bloqueando el sistema operativo y las aplicaciones para evitar el peligro?**
- **¿Nuestros usuarios manipulan la configuración y ponen en riesgo los sistemas corporativos?**
- **¿Cómo podemos evitar el cruce de datos personales y profesionales en los dispositivos de uso compartido?**
- **¿Nos centramos mucho en las PC? ¿Qué pasa con los teléfonos y las tablets?**
- **¿Cómo nos aseguramos de que los dispositivos de los clientes dispongan de seguridad y parches apropiados?**
- **¿Cómo nos aseguramos de que los empleados sigan las reglas y no aumenten el riesgo por negligencia o actividades maliciosas?**
- **¿Cómo secundamos y administramos los dispositivos personales? ¿Dónde trazamos la línea entre la responsabilidad profesional y personal?**

En muchos sentidos, el endpoint es la parte más difícil de administrar de la pila tecnológica del trabajo remoto. La división de la propiedad personal y las operaciones corporativas se basa en el compromiso de ambas partes, lo que está en contra de los principios generales de la seguridad de TI. También es la razón por la que un 20 % de los intentos de piratería está dirigido a los dispositivos de los usuarios finales[9].

Sin embargo, un 48 % de las empresas ya implementó políticas estrictas de acceso de usuarios y dispositivos, y otro 24 % está dispuesto a seguir su ejemplo el próximo año[10]. Es posible que estas organizaciones desplieguen dispositivos corporativos o sesiones de VDI a sus usuarios en lugar de continuar con los dispositivos personales que conllevan un mayor riesgo.

Antimalware

Cada dispositivo de endpoint que se conecta a los recursos corporativos se debe asegurar con una herramienta antimalware. Es importante evitar que los virus y ransomware entren a la red para contener la propagación y evitar el daño potencial ya que, por ejemplo, un 27 % de los incidentes de seguridad se debe al ransomware[11]. Por sorpresa, un 91 % de los trabajadores remotos mencionó en una encuesta que su empleador **no** les proporcionó una solución de antivirus para instalarla en sus dispositivos personales que utilizaron para trabajar[12].



Son esenciales las herramientas antimalware inteligentes que emplean la heurística avanzada y el aprendizaje automático para identificar y bloquear automáticamente los archivos y la actividad que resulten sospechosos. Estas herramientas proactivas reducen de gran manera el riesgo, en particular cuando el equipo de seguridad de TI no siempre puede actualizar o controlar los dispositivos remotos de forma manual.

Phishing y suplantación

El phishing y las estafas por correo electrónico siguen siendo populares entre los ciberdelincuentes porque funcionan: un 22 % de los incidentes informados durante el 2020 involucró phishing[13]. La buena noticia es que la mayoría de las defensas de los correos electrónicos seguirán funcionando, sin importar de dónde accedan los trabajadores remotos a sus bandejas de entrada, ya que están alojadas en la red corporativa (o en la plataforma asegurada de la nube).

Sin embargo, cuando el empleado tiene un dispositivo de uso mixto, siempre hay un riesgo de que sea víctima de un correo electrónico de phishing o un archivo adjunto infectado de su cuenta personal. Al burlar las defensas corporativas, los hackers pueden conseguir datos y credenciales valiosos engañando a los empleados con un correo electrónico bien elaborado.

Una vez más, la instalación de antimalware en los equipos de escritorio ayudará, pero los empleados también deberían recibir una capacitación regular sobre cómo identificar y administrar el correo electrónico. Hay que animarlos a que apliquen sus conocimientos también al correo electrónico personal, entre otros, porque les permitirá no sufrir pérdidas a nivel personal.

Actualizaciones de endpoints y ejecución de parches

Otra preocupación importante será mantener los dispositivos conectados parchados y actualizados. No parchar los equipos es una invitación abierta para que los delincuentes se aprovechen.

Es posible que los trabajadores remotos deban volver a la oficina para someterse a "comprobaciones de estado" periódicas. O se necesitará establecer un horario para que los dispositivos se puedan actualizar durante la noche según una rutina acordada anteriormente.

En el futuro, es posible que la migración a un sistema de VDI alojado sea una mejor opción estratégica. Las imágenes centralizadas permanecen bajo su control en todo momento, y se pueden administrar y mantener de la misma manera que los dispositivos existentes en las instalaciones.

Comportamiento del usuario final

El comportamiento de los empleados siempre fue una de las mayores preocupaciones del trabajo remoto, por lo general en términos de productividad. Pero el comportamiento está al comienzo de las listas de preocupaciones de los líderes de TI, sobre el phishing, las contraseñas poco seguras, la poca seguridad de los endpoints y la TI invisible[14]. Aún peor, un 52 % de los administradores de TI confirma que los empleados encuentran soluciones alternativas a los sistemas y políticas de seguridad[15]. Por lo general, este no es un comportamiento malicioso, sino todo lo contrario: es el intento de los trabajadores de administrar barreras para tener una mayor eficiencia y productividad. No obstante, cada atajo que ahorra tiempo también es una amenaza potencial para la integridad del sistema.

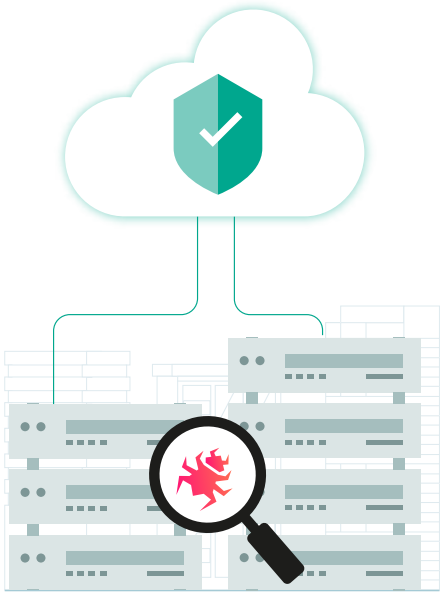
Este asunto es complicado si se trata de dispositivos de uso mixto de los empleados. Las empresas tendrán que negociar un compromiso con sus trabajadores sobre la forma en que interactúan con los sistemas corporativos, en especial cuando los usuarios gastaron una media de USD 348 de su propio dinero para actualizar o mejorar la tecnología mientras trabajan en casa debido a la COVID-19[16]. Una vez más, las infraestructuras de escritorios virtuales (VDI) o las sesiones locales de sandbox pueden proporcionar controles adicionales que impidan las soluciones alternativas sin sobrepasar el límite entre lo profesional y lo personal. El 93 % de las empresas cuenta con una política de seguridad para el trabajo remoto[17]: ahora necesitan hacer que se cumpla.

Confianza cero en el equipo de escritorio

A pesar de que la confianza cero se implementa en el nivel de la infraestructura, también cumple una función en el nivel de los endpoints. Los sistemas deben estar configurados para monitorear y verificar con cuidado la actividad remota a fin de controlar y limitar el acceso cuando sea necesario.

Los mecanismos de confianza cero ayudarán a resolver muchas de las incertidumbres relacionadas con los dispositivos "desconocidos". A los empleados remotos se les asigna un acceso con menos privilegios, lo que les asegura que puedan utilizar los recursos que necesitan para trabajar sin exponer otros sistemas que no necesitan. Los controles se pueden aplicar en el nivel del escritorio, la red y la infraestructura para contar con seguridad detallada y mayor protección de los recursos corporativos.

Sección 2: ¿Su infraestructura está en orden?



Para la mayoría de las empresas, la infraestructura central ya debería estar bien asegurada, al menos para uso interno. Sin embargo, el cambio al trabajo remoto dañó la seguridad del perímetro para entregar acceso a recursos centralizados.

A medida que sus capacidades de trabajo remoto se consolidan, su equipo de seguridad de TI debe plantear algunas preguntas difíciles:

- **¿Deberíamos migrar a los trabajadores remotos a una configuración de VDI?**
- **¿Existen aplicaciones internas que podrían estar mejor aseguradas si se migran a una alternativa alojada en la nube/SaaS?**
- **¿Cómo controlamos el acceso a los recursos internos?**
- **¿Cómo se protegen los datos, en particular si se almacenan fuera del perímetro de red?**
- **¿Cómo podemos mitigar los efectos del malware y ransomware?**

Retención de los datos dentro de la red

Si se mantienen los sistemas y los datos dentro de la red corporativa, se reduce inmediatamente el riesgo de pérdida, robo o filtración. El uso de soluciones de VDI proporciona a sus usuarios finales una experiencia similar a la de un equipo de escritorio y garantiza que los datos permanezcan dentro de su infraestructura de cliente ligero; no hay necesidad de transferir archivos o datos al dispositivo local, donde corren un mayor riesgo de verse comprometidos.

Uso de la capacidad de la nube

Las aplicaciones basadas en la nube y el SaaS suelen estar protegidos por defensas de seguridad de clase empresarial. Puede que sea más apropiado y eficaz migrar las aplicaciones fuera del centro de datos local. Además de simplificar el acceso remoto a estas aplicaciones, la habilitación en la nube puede aumentar la seguridad general de sus datos.

Fortalecimiento del control de la cuenta

Las contraseñas siguen siendo una fuente continua de problemas: las empresas sufren una media de 922 331 intentos de robo de credenciales cada año[18], mientras que el 37 % de las infracciones implica credenciales robadas[19]. Siempre fue difícil mantener la seguridad de las contraseñas en el perímetro de red. Pero los endpoints remotos simplemente aumentan el riesgo de que se expongan o roben credenciales. La actualización de los controles de cuentas para utilizar el inicio de sesión único (SSO) y la autenticación de varios factores (MFA) o las alternativas sin contraseña ofrece una capa adicional de protección si las credenciales se ven comprometidas.

Puede fortalecer aún más las defensas utilizando la autenticación continua y el análisis de anomalías. Estas herramientas monitorean la actividad del usuario para identificar y bloquear automáticamente el comportamiento sospechoso a fin de limitar el daño en el caso de vulneraciones exitosas.

Uso compartido de archivos

Además de poder acceder a los datos con facilidad, los trabajadores remotos deben ser capaces de colaborar con sus colegas. Existe un gran riesgo de que los usuarios se decanten por cuentas personales en plataformas como Dropbox o Google Drive, lo que deja esos datos fuera de su control y aumenta el riesgo de exposición.

Tendrá que identificar e implementar sistemas de intercambio de archivos aprobados para los trabajadores remotos, incluidas las versiones de pago y controladas de forma centralizada de servicios como Dropbox y Google Drive. Sus disposiciones para compartir archivos deben aplicar el cifrado a todos los datos en tránsito y en reposo.

Puede proteger aún más los datos utilizando un agente de seguridad de acceso a la nube (CASB). El CASB actúa como un proxy para aplicar políticas a los datos a medida que se transfieren desde y hacia la nube. De este modo, puede asegurarse de que los datos se utilicen de forma responsable desde cualquier dispositivo, incluidos los teléfonos y tablets personales no administrados.

Bóveda de datos

El ransomware representa una amenaza real e importante para todos sus sistemas. Una infección no controlada puede dejar fuera de servicio los sistemas de producción y las copias de seguridad, lo que hace casi imposible la recuperación total.

La bóveda de datos, con el uso de copias de seguridad inmutables, evita que se cifren los archivos. Esta es una capa de protección importante en el caso de que los usuarios remotos inevitablemente introduzcan ransomware en la red.

Adopción de una postura de confianza cero

Quizás el cambio estratégico más importante que su empresa debe hacer en la era del trabajo remoto es la adopción de una postura de seguridad de confianza cero. Según las directrices publicadas por la Agencia de Seguridad Nacional de Estados Unidos, el modelo de seguridad de confianza cero funciona según tres principios básicos:

1. **Nunca confiar, siempre verificar**: trate a todos los usuarios, dispositivos, aplicaciones, cargas de trabajo y flujos de datos como no confiables. Autentique y autorice explícitamente a cada uno con el menor privilegio requerido mediante políticas de seguridad dinámicas.

2. **Asumir las vulneraciones**: opere y defienda los recursos con conciencia asumiendo que un adversario ya está presente en el entorno. Deniegue por defecto y analice minuciosamente todos los usuarios, dispositivos, flujos de datos y solicitudes de acceso. Registre, inspeccione y monitoree continuamente todos los cambios de configuración, los accesos a los recursos y el tráfico de red para detectar actividades sospechosas.

3. **Verificar explícitamente**: el acceso a todos los recursos se debe realizar de una manera consistente y segura utilizando varios atributos (dinámicos y estáticos) a fin de obtener niveles de confianza para las decisiones de acceso contextual a los recursos[20].

La utilización de los principios de la confianza cero ayudará a identificar y mitigar los problemas más rápido, como también a diseñar una infraestructura más segura para sus trabajadores remotos. El monitoreo va más allá de la simple evaluación de la actividad de los usuarios; se evalúa cualquier operación o interacción para identificar los errores de configuración junto con los intentos de piratería activos.

Sección 3: ¿Su red está en orden?

Sus usuarios necesitan una conectividad segura y confiable a fin de asegurar que puedan acceder a los recursos corporativos para trabajar. El despliegue de las conexiones VPN es relativamente sencillo, pero la administración, el mantenimiento y la vigilancia de estas suponen una importante carga administrativa.

A fines de ayudar a evaluar si su red está asegurada de forma adecuada para el trabajo remoto, debe saber lo siguiente:

- **¿Están aseguradas todas las conexiones entrantes y salientes de los dispositivos de nuestros trabajadores remotos?**
- **¿Cómo enfrentamos el phishing y los sitios web falsos?**
- **¿De qué manera nuestros usuarios finales acceden a Internet?**
- **¿Qué amenazas existen dentro de las oficinas en casa de nuestros usuarios?**

La conexión entre el usuario final y los recursos corporativos es otro punto débil clave en sus disposiciones de trabajo remoto.

Cifrado de conexiones

Las conexiones de redes privadas virtuales (VPN) son ahora un método de conectividad estándar, utilizado por un 72 % de las empresas para garantizar el acceso a la red corporativa[21]. Al cifrar el tráfico entre endpoints, puede evitar los ataques más comunes de espionaje. En el futuro, debe asegurarse de que se apliquen niveles similares de cifrado a todos los recursos remotos, lo cual incluye las plataformas en la nube y el SaaS.

Sin embargo, una pequeña nota para tener en cuenta: solo un 43 % de los trabajadores remotos encuestados señaló que utilizaba una VPN cuando trabajaba desde casa[22]. Es probable que muchos usuarios no sepan que sus conexiones están cifradas. Por el contrario, indica una falta de formación y conocimientos en materia de seguridad básica que los ayudaría a desempeñar su papel para proteger mejor la empresa.

Secure Access Service Edge (SASE)

Las VPN son útiles para asegurar las conexiones entre los endpoints y el centro de datos corporativo, pero la red moderna hace un uso intensivo de activos distribuidos como los servicios en la nube. La tecnología de Secure Access Service Edge unifica la tecnología WAN con los servicios de seguridad de red como CASB (ver más arriba), Firewall as a Service y confianza cero en un panel de control centralizado.

SASE se suministra como un servicio en la nube para monitorear la identidad de la entidad, proporcionar un contexto en tiempo real y aplicar las políticas de seguridad y cumplimiento normativo de la empresa y la evaluación continua del riesgo/confianza a lo largo de las sesiones. SASE es flexible, escalable y capaz de proteger los activos de datos en las instalaciones, en la nube y en cualquier punto durante el tránsito.

Filtro de solicitudes

Las aplicaciones antivirus de endpoints suelen detectar y bloquear las solicitudes de red sospechosas, pero ¿qué ocurre si el usuario final desactiva las protecciones locales? La activación del filtro de DNS proporciona una capa adicional de seguridad de la red, lo que impide que el malware realice llamadas y reduce el riesgo de que los usuarios sean engañados para visitar sitios maliciosos.

Políticas de Wi-Fi

El trabajo remoto no siempre se limita a la oficina en casa. Los espacios compartidos de trabajo e incluso las cafeterías se consideran ahora lugares de trabajo viables para sus empleados. Sin embargo, la posibilidad de que se produzcan ataques de intermediario y otros ataques de secuestro de conexiones es un riesgo grave para la seguridad.

La conectividad VPN por defecto proporcionará cierta protección, pero también debe educar a los usuarios sobre el uso seguro de las redes Wi-Fi públicas, si es posible, y elaborar políticas en consecuencia.

Uso de la red doméstica

En la era de la automatización del hogar controlada en la nube, las redes domésticas de sus usuarios también son cada vez más inseguras. Cuando se trabaja desde casa, su empresa tiene muy poco control directo sobre la red compartida, la cual se podría utilizar para afectar los dispositivos corporativos conectados, a menudo, a través de dispositivos IoT que están mal protegidos.

Debe invertir en tecnologías que fortalezcan los dispositivos locales para que tengan una mejor defensa contra malware local, ataques externos y otros exploits que podrían utilizarse para conectarse a la red corporativa. La mayoría de los enrutadores Wi-Fi domésticos ahora ofrecen capacidades de doble red; animar a los trabajadores remotos a configurar y utilizar la red secundaria para segregar el tráfico personal y profesional ayudará a evitar el cruce. Solo un 7 % de las empresas utiliza este método en la actualidad, lo que representa una importante oportunidad desaprovechada para mejorar la seguridad de extremo a extremo[23].

Conclusión: fortalecimiento de su estrategia de seguridad de trabajo remoto

Como vimos, la seguridad eficaz para el trabajo remoto es un proceso de tres partes. Su estrategia debe abarcar la infraestructura, la red y los dispositivos utilizados por los empleados para acceder a los recursos corporativos.

El uso de dispositivos personales crea un desafío doble. En primer lugar, hay que responder a las preocupaciones de los empleados que pueden sentir que se está infringiendo su privacidad y autonomía. A continuación, hay que identificar una forma de administrar y controlar una red en constante ampliación que opera fuera de los controles existentes.

El enfoque orgánico de la implementación del trabajo remoto es intrínsecamente inseguro y no escalable. En el futuro, las empresas tendrán que reforzar sus defensas en todos los niveles: centro de datos, red y endpoint. Las herramientas como CASB y la confianza cero ayudan a resolver algunos de estos problemas, al igual que los esfuerzos por estandarizar las aplicaciones y herramientas que utilizan los empleados remotos.

De cara al futuro, SASE será crucial, ya que permitirá a las empresas ampliar la seguridad a medida que cambien sus exigencias. La adopción es muy baja en la actualidad (aproximadamente un 1 %[24]), pero se espera que se acelere rápidamente a medida que las organizaciones consoliden los conjuntos de herramientas para simplificar la administración y la cobertura de la seguridad. La seguridad alcanzará por fin la ubicuidad y protegerá los sistemas y los activos de forma coherente, sin importar su ubicación. Y, cuando esto ocurra, la diferencia entre el trabajo remoto y las operaciones en la oficina, desde el punto de vista de la seguridad, será insignificante.

¿El trabajo remoto disuelve su perímetro corporativo? ¿Demasiadas tareas urgentes y tiempo insuficiente para realizarlas? ¿Desea (y necesita) la EDR, pero le preocupa la complejidad? En Kaspersky podemos ayudar a afrontar estos retos.

Ya sea que quiera fortalecer las defensas internas o combatir las amenazas más recientes con una orientación de expertos externos, Kaspersky puede ayudarle. Nuestra solución Kaspersky Optimum Security basada en la nube le permite actualizar la protección contra amenazas nuevas, desconocidas y evasivas mediante la detección y respuesta eficaces contra amenazas y la supervisión de seguridad ininterrumpida, sin costos prohibitivos ni complejidad. Más visibilidad. Más potencia. Más control.

Obtenga más información en go.kaspersky.com/es_mx_optimum

Lectura recomendada:

[Aprendizaje automático en ciberseguridad]
[Cómo saber qué nivel de protección de endpoints necesita]
[Guía del comprador de EDR]
[Impulse la ciberseguridad de los equipos de trabajo remoto con el fortalecimiento del sistema]

---

[1] ISC Cybersecurity Workforce Study 2021, (ISC)2: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[2] Business and individual attitudes towards the future of homeworking, UK: April to May 2021, Office for National Statistics: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/businessandindividualattitudestowardsthefutureofhomeworkinguk/apriltomay2021
[3] The Flexible Revolution: Are You Ready?, OpenVPN: https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[4] 2021 Remote Workforce Security Report, Cybersecurity Insiders: https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[5] Zoom security issues: Everything that's gone wrong (so far), Tom's Guide: https://www.tomsguide.com/news/zoom-security-privacy-woes
[6] 2021 Remote Workforce Security Report, Cybersecurity Insiders: https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[7] COVID-19 Cybersecurity in the Remote Workforce, PC Matic: https://www.pcmatic.com/news/covid-19/
[8] 2021 Remote Workforce Security Report, Cybersecurity Insiders: https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[9] 2020 Data Breach Investigations Report, Verizon: https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[10] Digital Distancing: Why remote working demands better cybersecurity in a changed world, Computing: https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[11] 2020 Data Breach Investigations Report, Verizon: https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[12] COVID-19 Cybersecurity in the Remote Workforce, PC Matic: https://www.pcmatic.com/news/covid-19/
[13] Ibid.
[14] Digital Distancing: Why remote working demands better cybersecurity in a changed world, Computing: https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[15] 2021 Remote Workforce Security Report, Cybersecurity Insiders: https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[16] People are Working More by Not Going to Work, but Worry about Home Tech, Data Security and Personal Costs, Lenovo: https://news.lenovo.com/pressroom/press-releases/new-lenovo-research-people-are-working-more-by-not-going-to-work-but-worry-about-home-tech-data-security-and-personal-costs/
[17] The Flexible Revolution: Are You Ready?, OpenVPN: https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[18] 2020 Data Breach Investigations Report, Verizon: https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[19] 2020 Data Breach Investigations Report, Verizon: https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[20] Embracing a Zero Trust Security Model, National Security Agency: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[21] Digital Distancing: Why remote working demands better cybersecurity in a changed world, Computing: https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[22] COVID-19 Cybersecurity in the Remote Workforce, PC Matic: https://www.pcmatic.com/news/covid-19/
[23] Ibid.
[24] Hype Cycle for Enterprise Networking, 2020, Gartner: https://www.gartner.com/en/documents/3987266

latam.kaspersky.com

kaspersky PREPARADOS PARA EL FUTURO