Lista de verificación: protección contra ransomware en la era del trabajo flexible

kaspersky PREPARADOS PARA EL FUTURO

El ransomware sigue siendo una amenaza creciente para cualquier organización, y una estimación sugiere que un 15,45 % de todos los usuarios de Internet sufrió al menos un ataque de malware en 2021[1]. No es de extrañar que la ciberseguridad sea una prioridad estratégica cada vez más importante para las empresas.

El riesgo de infección por ransomware aumentó en los últimos años, sobre todo porque la adopción del trabajo remoto se aceleró en respuesta a los controles de la pandemia. Las investigaciones sugieren que la prisa por lo remoto hizo que muchas organizaciones redujeran la supervisión o aflojaran muchos de sus protocolos de seguridad habituales.

Cuando se trata de ransomware, la mayor parte de la atención se centra en restablecer el acceso a los datos cifrados lo antes posible. Sin embargo, vale la pena recordar que los ciberdelincuentes suelen exfiltrar archivos con fines de chantaje adicional, con el fin de exigir más pagos para evitar la filtración de información confidencial.

En 2021, menos empresas implementaron herramientas de seguridad de red (un 5 % menos) o de monitoreo del usuario final (un 6 % menos)[2]. Sin un monitoreo y una seguridad eficaces de los endpoints, el riesgo de convertirse en víctima del ransomware aumenta considerablemente.

Los endpoints siempre fueron un punto débil en la seguridad corporativa, ya que, a menudo, eran las superficies de ataque más fáciles disponibles para los hackers. Pero las prácticas de trabajo remoto trasladaron esos endpoints **fuera** del perímetro de la red, lo que hace aún más difícil administrar y mitigar la seguridad. La proliferación de endpoints ofrece a los atacantes una mayor selección de objetivos potenciales, lo que aumenta aún más sus posibilidades de éxito.

Para evitar un brote importante de ransomware, se debe aplicar una estrategia eficaz que funcione en varios niveles diferentes. A medida que el trabajo remoto se convierte en un aspecto rutinario de las operaciones, las organizaciones deben perfeccionar y reforzar sus protecciones de los endpoints, especialmente respecto a la forma de detectar y bloquear las infecciones de ransomware.

Esta guía sirve como lista de verificación práctica, que lo ayuda a evaluar qué tan bien protegido está contra el ransomware en el borde de la red y dónde debe mejorar sus defensas, lo que incluye lo siguiente:

- **1. Detección del ransomware de endpoints**
- **2. Configuración de endpoints**
- **3. Disposiciones de copias de seguridad**
- **4. Operaciones de descarga**
- **5. Capacitación de usuarios finales**
- **6. Planificación de respuesta ante incidentes**

[1]Kaspersky Security Bulletin 2021. Statistics, Kaspersky: https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/

[2]Cyber Security Breaches Survey 2021, UK Department for Digital, Culture, Media & Sport: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Detección del ransomware de endpoints

Es muy importante detener al ransomware antes de que prolifere. Mientras más rápido se detecte y bloquee una infección, menos daños e interrupciones causará.

Por lo general, su organización puede detectar el malware enviado por correo electrónico directamente a los empleados en el servidor de correo, pero esto no impide que se los engañe para que descarguen ejecutables externos con un mensaje de spear phishing bien elaborado.

Puede mejorar su capacidad de detección de ransomware mediante el bloqueo de los ejecutables sospechosos en el endpoint:

- **Implemente un conjunto sólido de herramientas antimalware para identificar y eliminar los ejecutables sospechosos antes de que puedan cifrar los archivos confidenciales.**
- **Utilice las capacidades de aprendizaje automático de las herramientas de detección y respuesta de endpoints (EDR) para identificar y bloquear de forma automática la actividad sospechosa del sistema.**
- **Considere la posibilidad de adoptar una solución de detección y respuesta administradas (MDR) para automatizar y acelerar los esfuerzos de mitigación del ransomware.**

La implementación de estas herramientas ayudará a contener una infección, lo que evitará que se propague a otros almacenamientos de archivos y sistemas.

Cabe señalar que los organismos federales y las agencias gubernamentales están endureciendo su postura sobre la forma en que las víctimas responden a las infecciones de ransomware. En 2019, el Departamento Especializado en Delitos en Internet del FBI (IC3) instó a las empresas a no pagar rescates[3].

Kaspersky respalda este consejo: "No pague. Cada pago de rescate representa una contribución financiera al desarrollo de malware y una señal para los ciberdelincuentes de que el esquema es rentable. Y es posible que no funcione, que no consiga nada aunque cumpla las indicaciones".[4]

La Oficina Federal Alemana de Seguridad de la Información (BSI) brinda un consejo claro: "La mejor protección contra las peticiones de rescate de los ciberdelincuentes es la aplicación consistente de medidas de seguridad informática".[5]

La implementación coherente de las medidas de TI implica mantener protecciones de los endpoints **fuera** del perímetro de la red similares a las del interior, en este caso, herramientas antimalware eficaces y fiables, y EDR inteligentes que puedan detectar actividades similares al ransomware de forma automática.

2. Configuración de endpoints

La configuración de endpoints también ayudará a reducir el efecto potencial de una infección de ransomware. Para los dispositivos proporcionados por la empresa:

- Utilice la lista de permisos del directorio de aplicaciones para garantizar que los empleados solo puedan ejecutar el software autorizado. Con la restricción adecuada, no pueden instalar aplicaciones, lo que reduce la posibilidad de poner en funcionamiento ejecutables infectados.
- Asegúrese de que las herramientas de seguridad de endpoints y cualquier otro software instalado estén configurados para actualizarse automáticamente con el fin de bloquear nuevas amenazas y cerrar posibles vulnerabilidades antes de que se puedan explotar[6].

Las prácticas recomendadas de seguridad sugieren aplicar las actualizaciones de software dentro de los 14 días siguientes a su lanzamiento. Lamentablemente, solo un 43 % de las empresas logra este objetivo[7]. Ya que son relativamente fáciles de implementar, esta es una oportunidad importante perdida para evitar la propagación del ransomware.

[3]High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI Internet Crime Complaint Center: https://www.ic3.gov/Media/Y2019/PSA191002
[4]Five tips for protecting yourself from ransomware, Kaspersky: https://www.kaspersky.com/blog/ransomware-five-tips/41444/
[5]Ibid.
[6]Ransomware world in 2021: who, how and why, Kaspersky: https://securelist.com/ransomware-world-in-2021/102169/
[7]Cyber Security Breaches Survey 2021, UK Department for Digital, Culture, Media & Sport: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Los endpoints de BYOD presentan un desafío adicional porque su organización solo puede ejercer un control limitado sobre el dispositivo. En este modelo de operación, tiene algunas opciones:

- Animar a los empleados a instalar una herramienta antimalware aprobada en cada uno de sus dispositivos. Proporcionar este software de forma gratuita es un buen incentivo porque protegerá los datos personales del empleado y los activos de la empresa.
- Protege los datos y aplicaciones corporativas con sandbox para que se mantengan separados de las aplicaciones personales. Si un empleado accede a un malware utilizando sus aplicaciones personales, el sandbox proporciona cierta medida de protección contra la propagación.

En última instancia, la protección de los dispositivos personales de los usuarios será un proceso de compromiso en el que se acuerda la implementación de medidas que sean convenientes para la empresa y el empleado. En el caso de que esto no sea posible, su empresa tendrá que considerar la posibilidad de brindar métodos de acceso alternativos o proporcionar a los empleados dispositivos propios.

3. Disposiciones de copias de seguridad

Una vez que se cifraron los archivos, hay dos opciones: pagar el rescate o recuperar copias "limpias" de los archivos de la copia de seguridad. Esto significa también tener una rutina de copias de seguridad sólida y fiable para sus dispositivos de endpoint.

En una implementación ideal, los empleados no tendrían la opción de almacenar los datos corporativos de forma local. Pero la realidad es que probablemente guarden los documentos en la unidad local, a menudo en la carpeta de descargas o en el escritorio.

Al prepararse para un trabajo remoto más seguro, hay que tener en cuenta lo siguiente:

- **¿Qué probabilidad hay de que los datos corporativos se almacenen de forma local?**
- **¿Qué datos se guardan?**
- **¿Cuáles son los riesgos si estos archivos se cifran o se vuelven inaccesibles?**
- **¿Cómo podemos hacer una copia de seguridad de estos datos?**

Este es un gran desafío fuera del perímetro de la red. La forma de resolver el problema la decidirá su arquitectura técnica y, hasta cierto punto, las capacidades de TI del usuario final. Las opciones que se deben considerar son las siguientes:

- Sincronizar los datos de las carpetas seleccionadas con el almacenamiento en la nube u otro servicio remoto, en lo posible con copias de seguridad inmutables que no se puedan sobrescribir ni modificar.
- Realizar una copia de seguridad en un disco extraíble local.
- Confiar en la funcionalidad incorporada en el sistema operativo para crear copias de seguridad y puntos de restauración automáticos.

Ninguna de estas soluciones posibles es ideal porque existe la amenaza inherente de replicar el ransomware y los archivos cifrados en la copia de seguridad. Sin embargo, hay que encontrar una forma de capturar los datos almacenados de manera local, sobre todo para estar en conformidad con las obligaciones de cumplimiento normativo y protección de datos.

Nunca olvide que la copia de seguridad de los datos es su última línea de defensa contra los archivos cifrados por el ransomware. También tenga en cuenta que la copia de seguridad y la recuperación no protegerán su empresa contra las filtraciones de datos o el doxing. Los delincuentes pueden seguir exigiendo un rescate bajo la amenaza de exponer información confidencial. La única defensa frente a estos ataques contra la **confidencialidad** es evitar que los delincuentes accedan a sus endpoints.

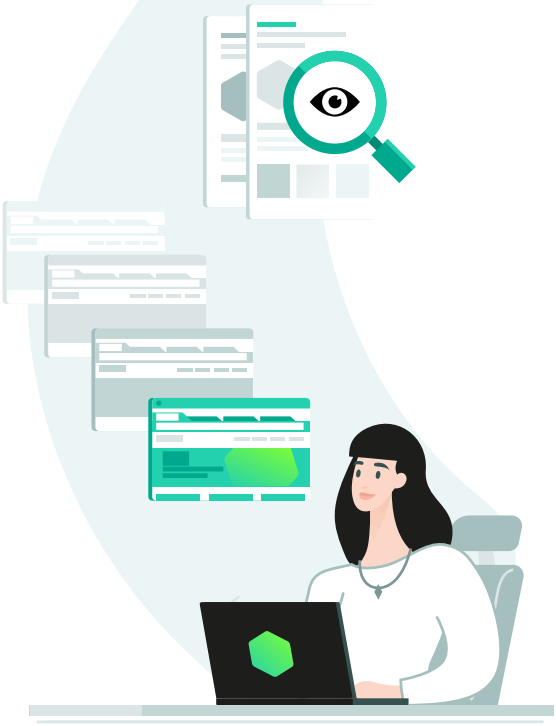
4. Operaciones de descarga

Mientras más datos y aplicaciones se guarden en un dispositivo de endpoints, más vulnerabilidades potenciales habrá para explotar. Y más atractivo se vuelve el equipo para los hackers. Por lo tanto, si se **reduce** la cantidad de aplicaciones y datos que se mantienen de forma local, menor será el impacto de una infección de ransomware.

Los servicios en la nube proporcionan una forma de descargar las aplicaciones, lo que minimiza la cantidad de datos que se almacenan en el dispositivo local. Hoy en día, el correo electrónico y las herramientas de productividad pueden ejecutarse como aplicaciones web en la nube, por ejemplo, para garantizar que se transfiera poco o nada a nivel local. Muchos, sobre todo los servicios de correo electrónico, ofrecen también protección avanzada contra el malware para examinar, detectar y bloquear los archivos adjuntos sospechosos antes de que sus usuarios puedan descargarlos.

La visualización ofrece otra posibilidad. Mediante la transmisión de las aplicaciones y el escritorio, los usuarios se pueden conectar a una sesión alojada en el centro de datos o la nube corporativos. La sesión alojada proporciona una sesión similar a la del escritorio para el usuario final, pero, una vez más, todos los datos y el procesamiento se completan dentro del sistema virtualizado.

Las sesiones de escritorio remoto (RDP) se consideran el mayor vector de ataque del ransomware[8]. Pero, cuando se configuran correctamente, se crea un sandbox útil entre el dispositivo de endpoint y los sistemas corporativos, como lo demuestra el amplio uso de RDP en la red corporativa.



Se pueden obtener los mismos beneficios para los trabajadores remotos reforzando la seguridad de endpoints, es decir:

- **Aplicar una política de contraseñas seguras para evitar los ataques de fuerza bruta.**
- **Implementar la autenticación de varios factores para evitar el secuestro de las sesiones.**
- **Utilizar conexiones VPN para todo el tráfico entre el endpoint y los servidores RDP.**
- **Evaluar y reforzar las reglas del firewall del perímetro de la red para evitar conexiones no autorizadas.**
- **Utilizar herramientas de seguridad EDR para evaluar la actividad con el fin de identificar y bloquear de forma automática las actividades sospechosas.**
- **Elegir puertos de conexión RDP no estándar para evitar intentos de piratería especulativa.**

En última instancia, la clave es evitar que los hackers y el malware comprometan la conexión y la sesión RDP, lo que significa asegurar el endpoint del usuario de forma adecuada.

5. Capacitación de usuarios finales

Los empleados son los activos más valiosos de cualquier empresa y pueden cumplir un rol fundamental en la prevención de la propagación de ransomware, siempre y cuando sepan qué hacer. Todos los empleados, no solo aquellos que trabajan de forma remota, deben recibir una capacitación regular a fines de que estén preparados para identificar ataques de ciberseguridad potenciales y saber qué deben hacer a continuación. Cada día, un 2 % de los empleados hace clic en un vínculo de phishing[9], y se pueden esperar cifras similares con respecto al ransomware.

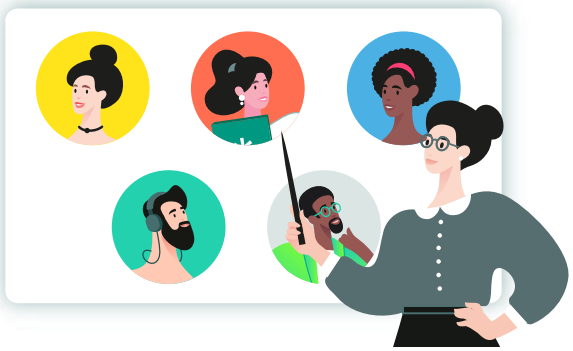
La capacitación debe ser interactiva, práctica y regular: al fin y al cabo, las amenazas a la ciberseguridad evolucionan constantemente. Una presentación puntual sobre la identificación de los correos electrónicos de phishing y los ejecutables sospechosos quedará obsoleta (y olvidada) en poco tiempo. Estos son algunos factores que se deben tener en cuenta a la hora de diseñar la capacitación en ciberseguridad para sus trabajadores remotos.

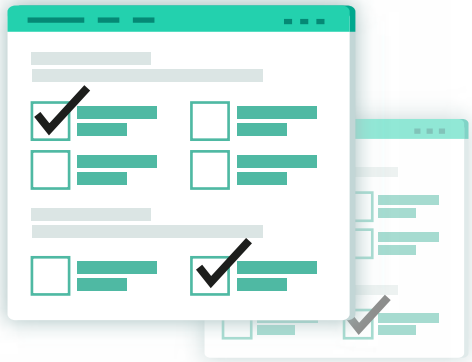
[8]How to secure RDP from ransomware attackers, Emsisoft: https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9]Mobile Security Index 2020 Report, Verizon: https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Adapte la capacitación

Los ataques de ransomware más eficaces se dirigen con cuidado a personas y funciones específicas. Así, es lógico que se debe adaptar la capacitación de la misma manera. Las finanzas, el marketing, los recursos humanos y los ejecutivos se enfrentarán a ataques ligeramente diferentes, por lo que capacitarlos en su propio "idioma" sobre las amenazas a las que probablemente se enfrenten será de mayor valor para ellos, y también resultará más eficaz para la empresa.



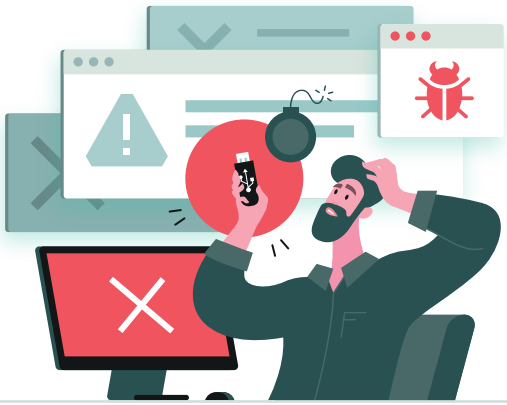


Ponga a prueba a sus empleados

El conocimiento tiene poco valor hasta que se pone en práctica, sobre todo cuando lo que está en juego es tan importante. Las pruebas rutinarias y periódicas garantizan que sus empleados puedan poner en práctica su capacitación cuando sea necesario. Las evaluaciones rutinarias también destacarán las lagunas de conocimiento o las oportunidades para mejorar sus habilidades y la postura de seguridad de su empresa.

Vaya más allá del phishing

El phishing y los archivos adjuntos maliciosos son la fuente potencial más obvia de infección de ransomware. Sin embargo, hay otros factores que sus usuarios finales deben tener en cuenta. Los discos extraíbles infectados, los sitios web maliciosos y la contaminación cruzada entre el trabajo y la actividad personal pueden introducir el malware en el endpoint y en la red corporativa más amplia. Debe asegurarse de que los empleados estén capacitados para que también se den cuenta de estos problemas potenciales.



Hágalo de manera entretenida (o interesante)

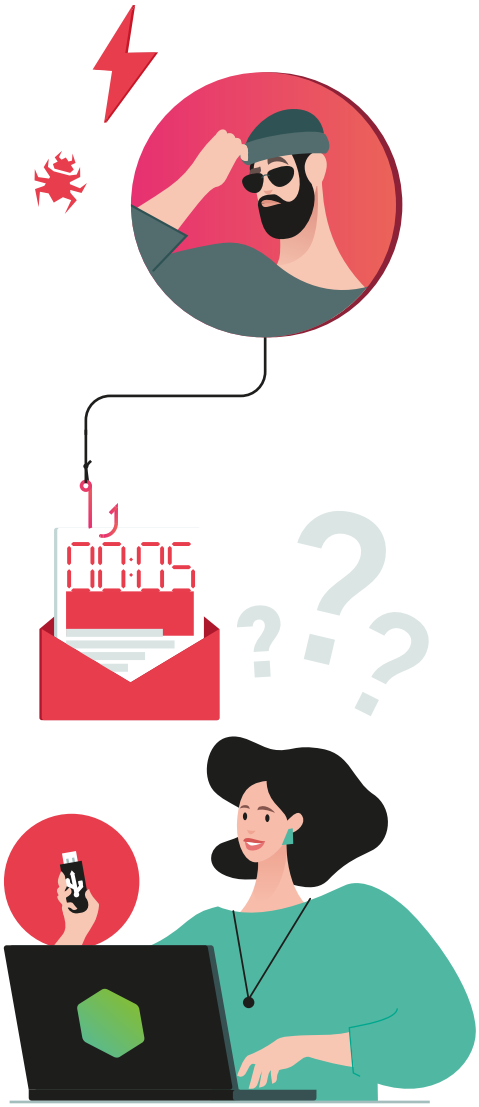
La ciberseguridad puede ser rutinaria y aburrida, sobre todo si no es su principal responsabilidad. Es muy poco probable que sus usuarios finales lean (o entiendan) los informes semanales del Sistema Nacional de Concienciación Cibernética de Estados Unidos, por ejemplo. El uso de la ludificación ayudará a aumentar el interés y el compromiso, especialmente a medida que los conceptos que se enseñan se vuelven más difíciles. Establecer objetivos y retos, fomentar la competencia y hacer que el proceso sea divertido animará a los empleados a mantenerse conectados y a seguir mejorando sus conocimientos y habilidades.

Invertir en sus usuarios finales es un paso importante para reforzar la defensa de sus endpoints. De hecho, disminuir los errores humanos es quizás la forma más eficaz de evitar el ransomware. También, ayudará a sus empleados a desempeñar un papel eficaz en las primeras etapas de una infección de ransomware, lo que contribuye a minimizar la propagación y el impacto general en la empresa.

6. Planificación de respuesta ante incidentes

Un asombroso 32 % de las empresas no tiene un plan formal de respuesta ante incidentes para hacer frente a incidentes de ciberseguridad como un brote de ransomware[10]. Estas organizaciones asumen un nivel de riesgo injustificable porque todas enfrentarán un incidente de malware en algún momento del futuro previsible.

Diseñar un plan de respuesta ante incidentes ayudará a su empresa a evaluar las vulnerabilidades y a tomar las medidas correctas para mitigarlas. El plan también le permitirá acelerar su respuesta, lo que es fundamental cuando se trata de un ransomware en el que cada segundo cuenta.



Aunque sea específico para su organización, todo plan de recuperación frente desastres (DR) de endpoints debe incluir lo siguiente:

- **Una estrategia de comunicación.** Hay que asegurarse de que la información correcta llegue a la parte interesada en el momento adecuado. Y también de que sus trabajadores remotos puedan conectarse con expertos que los ayuden en las primeras fases de una infección.
- **Un plan de ataque.** Decida cómo se determina la gravedad de un ataque y cómo responderá. ¿Pagará el rescate o intentará recuperar los datos de la copia de seguridad?
- **Documentación accesible.** Hay una probabilidad muy alta de que una infección de los endpoints impida a los empleados acceder a los manuales o las instrucciones de respuesta frente al ransomware. Debe asegurarse de que siempre haya una forma de obtener esta información, incluso si sus sistemas no funcionan.
- **Orientación para los empleados.** Apenas se detecte un problema, debe asignar a un especialista que pueda ayudar al trabajador remoto. Este puede guiar al usuario en los esfuerzos iniciales de mitigación y recuperación, y también recopilar información para incluirla en el informe para los reguladores si la situación lo amerita.
- **Vigilancia mejorada.** En cuanto se detecta una infección de ransomware en un endpoint remoto, su equipo de seguridad de TI debe aumentar los niveles de supervisión y notificación para evaluar si los sistemas centrales también se vieron comprometidos. Luego de esto, puede activar el plan principal de recuperación ante desastres si es necesario.

Con un plan de recuperación ante desastres bien diseñado, su empresa está mejor posicionada para reducir el impacto del malware y contener la propagación de manera ideal mucho antes de que llegue a los sistemas y datos esenciales.

[10]Cyber Security Breaches Survey 2021, UK Department for Digital, Culture, Media & Sport: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Conclusión

Los directivos de TI llevan muchos años preocupados por el trabajo remoto, y con razón. Sin embargo, los últimos acontecimientos cambiaron las operaciones para siempre, y el trabajo remoto ahora es un aspecto estándar de las empresas.

Al mismo tiempo, el ransomware se convirtió en una herramienta estándar en el kit de los ciberdelincuentes. Los ataques contra las organizaciones son frecuentes, eficaces y potencialmente devastadores. Con las superficies de ataque adicionales que proporcionan los trabajadores remotos, es muy probable que todas las empresas se vean afectadas en algún momento.

Por lo tanto, la protección de los endpoints contra el ransomware debe ser una prioridad estratégica. De lo contrario, puede ser demasiado tarde para que su empresa responda de manera eficaz cuando ocurra lo inevitable.

Los seis factores expuestos en este documento ayudarán a su empresa de manera inmediata a tener una mejor preparación para cuando llegue el ransomware. Si se abordan estos factores, se mejorará inmediatamente la postura de seguridad de los endpoints:

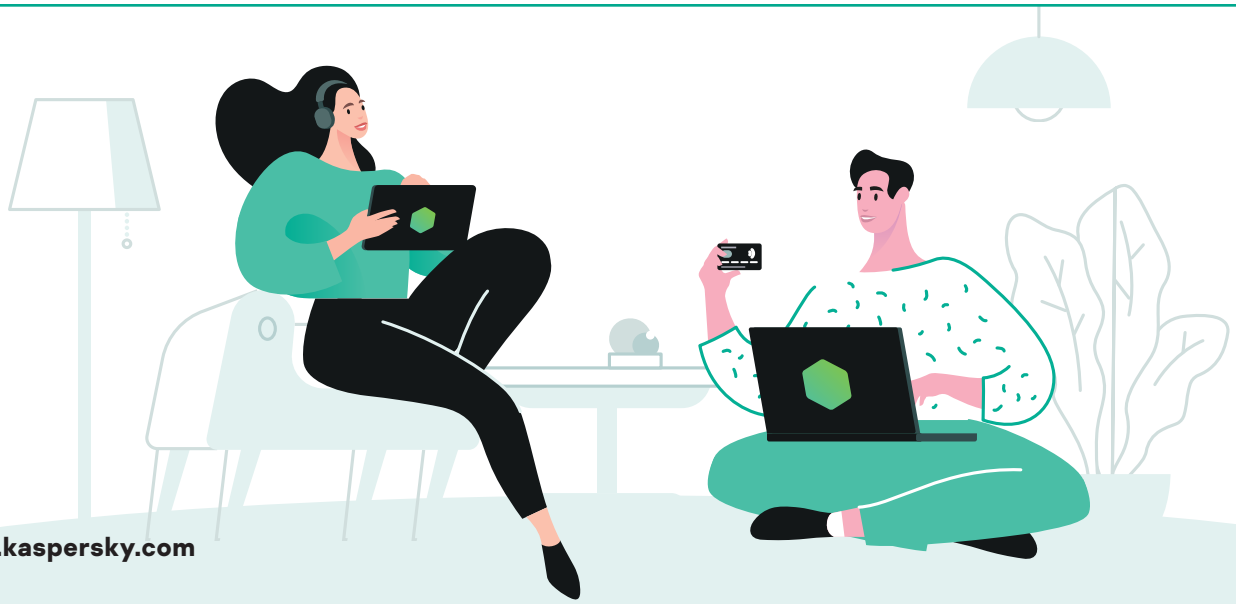
1. Detección y eliminación de malware
2. Configuración del dispositivo
3. Copia de seguridad y recuperación de los datos
4. Operaciones de descarga
5. Capacitación
6. Planificación de recuperación ante desastres

Si quiere obtener más información sobre cómo proteger a los trabajadores remotos y al resto de su organización contra el ransomware, Kaspersky puede ayudarlo. 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:

La historia del año: el ransomware en los titulares
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



latam.kaspersky.com

kaspersky PREPARADOS PARA EL FUTURO