

En general, calificamos a su organización como:

Políticamente



Detección



Respuesta



Recuperación

[Volver a tomar la evaluación](#)



Detectar

Cuando se trata de proteger proactivamente a su organización con las mejores prácticas de detección, está calificado como:

Políticamente

Vea el video para obtener un resumen.

Cannot load video.
This video is unavailable



Responder

Cuando se trata de responder de manera rápida y eficaz ante un incidente cibernético para limitar el daño o el impacto negativo, está calificado como:

Cannot load video.
This video is unavailable

Políticamente

Vea el video para obtener un resumen.



Recuperar

Cuando se trata de recuperar sus datos y reanudar las operaciones después de un incidente cibernético, está calificado como:

Políticamente

Vea el video para obtener un resumen.

Cannot load video.
This video is unavailable

Su informe personalizado sobre resiliencia cibernética

Gracias por tomar la autoevaluación de resiliencia cibernética de Dell Technologies elaborado por ESG. El objetivo de esta evaluación es ayudarlo a comprender cuán vulnerable es su organización al ransomware y otros sofisticados ataques cibernéticos en la actualidad, identificar áreas de vulnerabilidad y explicar lo que puede hacer para hacer frente a estos riesgos. Para ello, evaluamos la preparación de su organización en tres áreas clave: la detección proactiva de amenazas, la respuesta ágil a las amenazas y la integridad de las funcionalidades de recuperación.

Según sus respuestas a la evaluación en cada una de estas áreas, categorizamos a su organización como **Políticamente**. Este es el nivel **más bajo** de preparación en esta evaluación. Las siguientes páginas detallan por qué su organización recibió esta calificación e incluyen recomendaciones para que su organización tenga en cuenta.



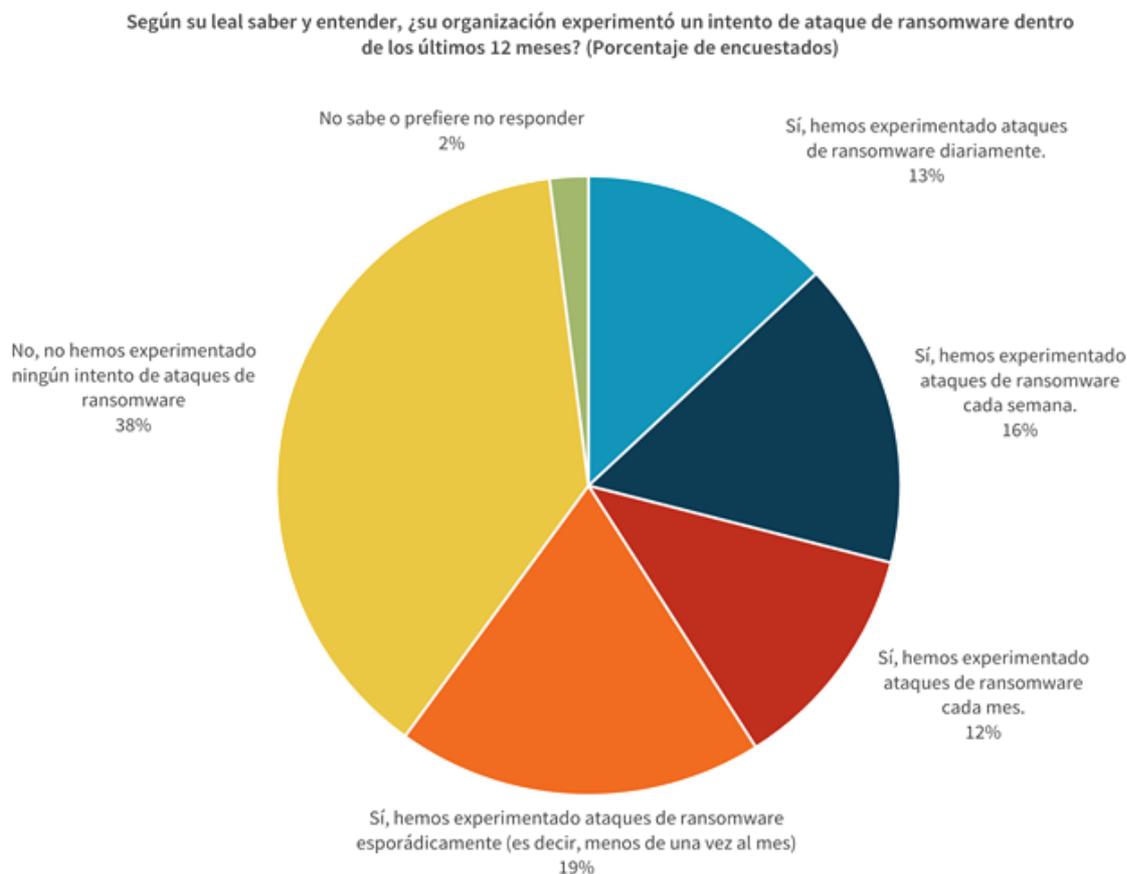
Detectar

El primer pilar de la evaluación se centra en la detección proactiva de amenazas, es decir, en las tecnologías y los procesos implementados en su organización para

detectar y prevenir un ataque cibernético o un incidente relacionado con ransomware. Teniendo en cuenta solo este pilar, su organización fue calificada como **Políticamente**, el nivel **más bajo** de preparación en esta evaluación.

- **Para comenzar la evaluación, preguntamos sobre las amenazas en las que se centra su equipo. Esto es importante porque, como demostró la investigación de las intenciones de gasto de ESG 2020, muchas organizaciones se encuentran bajo un constante bombardeo de ransomware y otras formas de ataques cibernéticos sofisticados (consulte la figura 1).** A medida que el panorama de amenazas se vuelve más complejo, los atacantes aprovechan múltiples vectores de ataque para comprometer y vulnerar a las organizaciones. Mientras que la mayoría de las organizaciones priorizan los ransomware y los ataques avanzados de varias etapas que involucran movimiento lateral, tanto la amenaza interna intencional como la involuntaria son preocupaciones crecientes para muchos. Se recomienda implementar soluciones de seguridad de terminales con protección confiable ante ransomware, junto con planes de respuesta ante incidentes y las estrategias de respaldo confiables con funcionalidades sin conexión para la protección, como las recomendadas por CISA. Si depende de un proveedor de servicios para proteger su organización, se recomienda encarecidamente tener conversaciones sobre estas áreas.

Figura 1



Fuente: ESG

- También le pedimos que considere la capacidad de su organización para cumplir con sus normas de cumplimiento.
- La evaluación se refirió a el uso de los marcos de riesgo de su organización para guiar su programa de seguridad.
- A continuación, la evaluación se refirió a la visibilidad de la red, la nube y terminales.
- Por último, la evaluación se centró en la eficacia de los controles implementados para prevenir un ataque de ransomware específicamente.



Respuesta

El segundo pilar de la evaluación se centra en la respuesta ágil antes amenazas, es decir, las tecnologías y los procesos implementados en su organización para responder ante un incidente de seguridad o ransomware rápidamente, de manera que limite su impacto. Teniendo en cuenta solo este pilar, su organización fue calificada como **Políticamente**, el nivel **más bajo** de preparación en esta evaluación.

- Le preguntamos cuál sería su respuesta más probable a un ataque exitoso de ransomware.
- A continuación, le preguntamos cuánto tiempo, esfuerzo y presupuesto ha asignado para proteger las copias de datos secundarias.
- Cuando se trata de la preparación para responder,
- Al llegar a las acciones de preparación específicas, la evaluación prioriza acciones como la planificación ante incidentes y las pruebas de recuperación.



Recuperación

El tercer y último pilar de la evaluación se centra en la integridad de las funcionalidades de recuperación. Es decir, las tecnologías y los procesos implementados en su organización para recuperar todos sus datos y permitir la reanudación de las operaciones normales de manera oportuna. Teniendo en cuenta solo este pilar, su organización fue calificada como **Políticamente**, el nivel **más bajo** de preparación en esta evaluación.

- Tener a las personas correctas en su lugar para recuperarse de un ataque cibernético es fundamental.

Figura 2

¿En cuál de las siguientes áreas cree que su organización de TI actualmente tiene una escasez problemática de habilidades existentes? (Porcentaje de encuestados, se permiten respuestas múltiples)



Fuente: ESG

- **Le preguntamos cuántos de sus datos cree que sería capaz de recuperar en caso de un ataque.**
- **La evaluación aborda la inversión de su organización en una infraestructura aislada o con air gap para copias de datos cruciales.**
- **Por último, independientemente de si su organización tiene una infraestructura aislada, le preguntamos cuántos de sus datos cree que deben protegerse en ese tipo de entorno.**

De qué manera Dell Technologies puede ayudar

Dell Technologies se esfuerza por construir un mundo confiable, seguro y conectado. Trabajamos incansablemente para tener siempre presente los datos, la red, la organización y la seguridad de los clientes, con la resiliencia cibernética y la seguridad diseñadas de manera integral en todos nuestros productos, soluciones y servicios. Desde las soluciones de Dell Endpoint Security y VMware Carbon

Black Cloud hasta Dell Trusted Devices y Dell EMC PowerProtect Cyber Recovery, lo ayudamos a crear y mantener una organización segura y resistente, incluso a medida que surjan nuevas amenazas.

En base a su evaluación y puntuación actual, hemos hecho recomendaciones por orden de prioridad para ayudar a mejorar su resiliencia. Nuestro [Centro de seguridad y confianza](#) brinda un fácil acceso a los recursos y las soluciones para ayudarlo a encontrar rápidamente las respuestas a sus preguntas sobre la seguridad para el consumidor y la empresa.

Desde el borde hasta el núcleo y la nube, nuestros expertos de la industria ofrecen orientación estratégica y funcionalidades prácticas probadas para ayudarlo a proteger su empresa y preservar su reputación ante las amenazas cibernéticas: confíe en Dell Technologies.

Cómo Dell puede ayudarlo a mejorar sus funcionalidades de detección:



- **Seguridad de terminales y dispositivos:** la cantidad de usuarios finales que trabajan de forma remota y móvil ha aumentado de manera exponencial. Con las brechas que ahora ocurren tanto por encima como por debajo del sistema operativo, necesita soluciones inteligentes que prevengan, detecten y respondan a las amenazas dondequiera que ocurran.
- **VMware Carbon Black™ Cloud:** los delincuentes cibernéticos constantemente actualizan las tácticas y oscurecen sus acciones dentro de las herramientas y los procesos comunes. Necesita una plataforma de terminales que le ayude a detectar las fluctuaciones menores que ocultan los ataques maliciosos y adaptar la prevención en respuesta.
- **Resiliencia proactiva de PowerEdge:** incorpore la confianza en su transformación digital con una infraestructura y un entorno de TI diseñados para interacciones seguras, además de la funcionalidad de anticipar las posibles amenazas.

Cómo Dell puede ayudarlo a mejorar su capacidad de respuesta:



- **Managed Detection and Response:** Manage Detection and Response con tecnología de Secureworks® Taegis™ XDR aprovecha el análisis y la experiencia avanzados para investigar peligros potenciales y una corrección en caso de que se identifique una amenaza.
- **Servicios de resiliencia empresarial:** Dell Technologies Services permite que las organizaciones sean altamente resilientes, ya que su negocio depende más de los servicios de TI basados en la nube, además de aumentar la presión de las partes interesadas y los reguladores.
- **Cyber Recovery Services:** Dell Technologies Services permite a las organizaciones aumentar su resiliencia cibernética a través de un programa holístico de recuperación cibernética que reúne la tecnología, el

proceso y el personal para formar una última línea de defensa para su organización.

Cómo Dell puede ayudarlo a mejorar su recuperación ante un ataque:



- **Power Protect Cyber Recovery:** PowerProtect Cyber Recovery protege y aísla los datos cruciales de ransomware y otras amenazas sofisticadas para que pueda recuperar datos exactos conocidos y reanudar las operaciones normales de la empresa con confianza.
- **Servicios de resiliencia empresarial:** Dell Technologies Services permite que las organizaciones sean altamente resilientes, ya que su negocio depende más de los servicios de TI basados en la nube, además de aumentar la presión de las partes interesadas y los reguladores.
- **PowerScale con Superna Eyeglass Ransomware Defender:** Superna Eyeglasses® Ransomware Defender es una solución de procesamiento de eventos en tiempo real altamente escalable que emplea análisis de comportamiento del usuario para detectar y detener un ataque de ransomware.

ESG, una división de TechTarget, es una empresa de análisis, investigación, validación y estrategia de TI que ofrece inteligencia del mercado e información útil a la comunidad mundial de TI.