

RESUMEN DE ESTUDIO DE ESG

Ciberresiliencia y rendimiento para el usuario final

Fecha: Marzo de 2022 **Autor:** Dave Gruber, analista jefe de ESG

RESUMEN: La ciberresiliencia es un requisito esencial para cualquier empresa. Dado que ahora y por tener usuarios trabajando desde cualquier parte, las organizaciones se enfrentan a mayores superficies de ataque, las empresas deben invertir en estrategias maduras para reducir el riesgo y liberar de cargas a los trabajadores. Un nuevo estudio de ESG señala que las inversiones en ciberresiliencia son aún más valiosas de lo que se creía: además de minimizar el riesgo, son fundamentales para innovar y prosperar en un mundo telemático.

Descripción general del estudio

Unas capacidades mejoradas de ciberresiliencia ayudan a reducir el riesgo. Pero ¿el nivel de madurez de la ciberresiliencia de una organización ayuda también a promover la innovación y a lograr un mayor éxito empresarial?

Para responder a esta pregunta, ESG realizó una encuesta a 750 responsables de la toma de decisiones de TI y, a continuación, segmentó a los encuestados en etapas de ciberresiliencia (consulte el gráfico a la derecha). Esta clasificación se basó en la manera en que los encuestados respondieron cuatro preguntas acerca de su organización. Cada una de estas preguntas representa las características de una organización Preparada (es decir, un atributo de una organización dotada de gran resiliencia) en cuanto a los equipos encargados de protegerla, la financiación de tecnologías para mitigar riesgos o el enfoque de la organización para minimizar riesgos de terceros.

- ¿Cómo describiría el nivel de dotación de personal en su equipo de ciberseguridad?
- ¿Cómo describiría el nivel de habilidades del equipo de ciberseguridad de su organización?
- ¿Cómo definiría la inversión de su organización en productos y servicios para proteger sus sistemas, aplicaciones y datos?
- ¿Su organización audita o inspecciona la seguridad de sus socios/proveedores de TI?

Niveles de madurez de ciberresiliencia



Solo se consideraron Preparadas aquellas organizaciones que comunicaron que no tenían vacantes pendientes en su equipo de seguridad, que su equipo de seguridad no tenía carencias de habilidades problemáticas, que financiaban tecnologías de seguridad a un nivel óptimo y que auditaban de manera formal y rigurosa los riesgos de terceros. Las organizaciones con 2 o 3 de estos atributos se consideraron Vulnerables, mientras que aquellas con 0 o 1 de estos atributos se consideraron Expuestas.

Según los datos, solo el 10 % de las organizaciones se clasificaron como organizaciones Preparadas con el mayor nivel de madurez de ciberresiliencia.

Al comparar el rendimiento tecnológico y empresarial tanto cuantitativa como cualitativamente en las cohortes encuestadas, el estudio validó que la mayor ciberresiliencia se correlaciona con un mejor tiempo de actividad del servicio de TI, una mayor rapidez en el descubrimiento y la respuesta a incidentes, un mejor tiempo de actividad del servicio de TI, una mayor satisfacción del usuario final, una innovación organizacional más ágil y una perspectiva empresarial más positiva. El estudio también proporciona un roadplan empírico que las organizaciones pueden seguir a fin de mejorar sus capacidades y resultados específicos. Este informe de estudio resumido se centra en las prácticas que las organizaciones deberían tener en cuenta para el entorno de los dispositivos de usuarios finales a fin de mejorar la madurez de la ciberresiliencia.

La seguridad de los dispositivos de usuarios finales y su impacto en las organizaciones ciberresilientes

ESG detectó varias diferencias clave entre las organizaciones Preparadas y las organizaciones con unos niveles más bajos de madurez de ciberresiliencia específica en lo que a su valor y el uso de la seguridad de dispositivos de usuarios finales en una plantilla moderna e híbrida respecta. En concreto, ESG observó lo siguiente:

- Las organizaciones preparadas tienen un **44 % más de probabilidades** de no informar de ninguna pérdida de datos debida a la puesta en peligro de los dispositivos en los últimos 12 meses (consulte la Figura 1).
- Las organizaciones preparadas tienen **casi el doble de probabilidades** que las organizaciones expuestas de informar de que menos del 1 % de sus usuarios ha sufrido un problema de seguridad que haya requerido el restablecimiento de los dispositivos. Como resultado, las organizaciones preparadas tienen un **44 % más de probabilidades** de no informar de ninguna pérdida de datos debida a la puesta en peligro de los dispositivos en los últimos 12 meses.
- De media, las organizaciones preparadas **reducen la cantidad de dispositivos desprotegidos un 33 %**.

Figura 1. Las organizaciones ciberresilientes sufren menos pérdidas de datos debidas a dispositivos en peligro

¿Cuántas veces en los últimos 12 meses ha sufrido su organización una pérdida de datos confidenciales o la fuga de datos confidenciales debido a una infección de malware u otro riesgo en portátiles y equipos de sobremesa? (Porcentaje de encuestados)



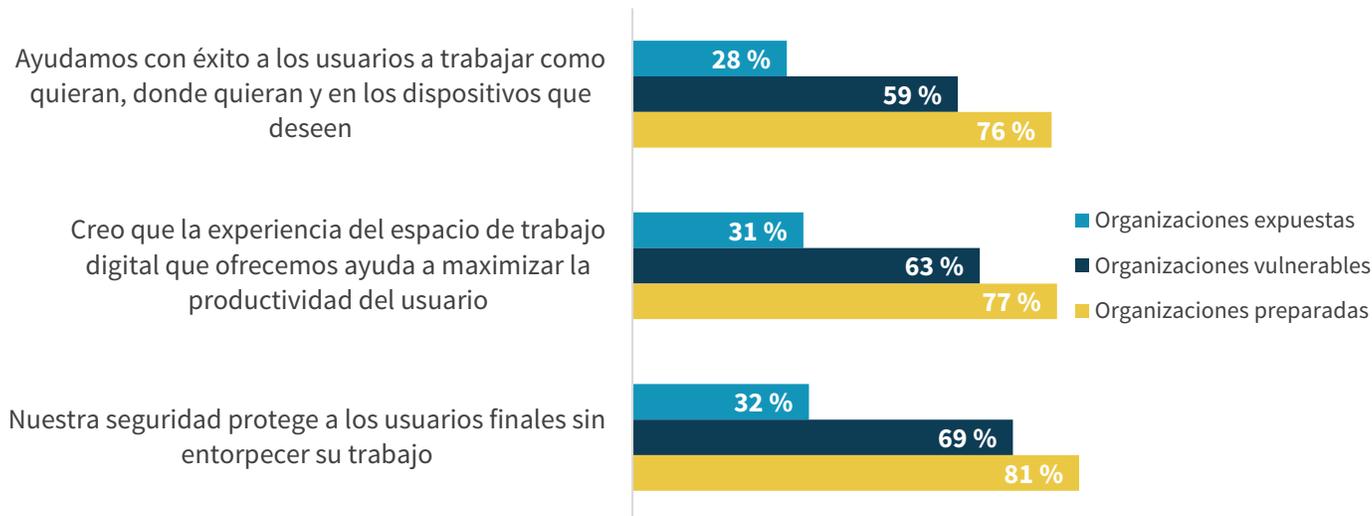
Fuente: ESG, una división de TechTarget, Inc.

Las organizaciones preparadas afirman que sus trabajadores están más satisfechos

Las organizaciones preparadas afirman que están haciendo un mejor trabajo al proporcionar a sus trabajadores la opción de trabajar donde y como decidan, lo que conlleva una mayor satisfacción en la experiencia de trabajo digital. En concreto, ESG descubrió que las organizaciones preparadas tienen **2,7 veces más probabilidades** de considerar que hacen un buen trabajo al permitir a los empleados trabajar en el lugar y con los dispositivos que elijan (consulte la Figura 2).

Figura 2. La ciberresiliencia genera trabajadores más productivos

Indique hasta qué punto está de acuerdo con las afirmaciones siguientes:
(Porcentaje de los encuestados que selecciona "Totalmente de acuerdo")



Fuente: ESG, una división de TechTarget, Inc.

El vínculo entre la ciberresiliencia y la satisfacción del usuario final

Si los empleados tienen la libertad de trabajar donde y como quieran sin impedimentos, pueden seguir centrados en los objetivos principales de la organización. El estudio revela que los trabajadores de las organizaciones preparadas otorgan a sus equipos de TI una **puntuación de satisfacción 5 veces mayor** que los usuarios de las organizaciones expuestas en lo relativo a la experiencia de trabajo digital (según una metodología NPS) (consulte la Figura 3).¹

Los usuarios de las organizaciones preparadas otorgan a sus equipos de TI una puntuación de satisfacción 5 veces mayor que los usuarios de las organizaciones expuestas.

¹ El 85 % de las organizaciones preparadas afirma que sus usuarios finales son "promotores", ya que otorgan una calificación de 9 o 10 al trabajo digital, mientras que el 0 % afirma que sus usuarios finales son detractores, lo que da como resultado un NPS +85 en la cohorte de las organizaciones preparadas. Y al contrario, solo el 29 % de las organizaciones expuestas afirma que sus usuarios finales son "promotores" y el 12 % detractores, lo que se traduce en un NPS +17 en la cohorte de las organizaciones expuestas.

Figura 3. La ciberresiliencia genera trabajadores más satisfechos

En términos generales, ¿cómo clasificaría en una escala de 0 a 10 el nivel de satisfacción de los usuarios finales en su organización con su experiencia general de espacio de trabajo digital?



Fuente: ESG, una división de TechTarget, Inc.

La mayor verdad

Las inversiones en ciberresiliencia son una necesidad debido a las funciones críticas que desempeñan los equipos de TI y de seguridad en toda la organización. Dado el creciente volumen de amenazas, la ciberresiliencia es ya una prioridad importante para todas las organizaciones.

No obstante, en este estudio de ESG se concluye que el valor de la ciberresiliencia proporcionado a través de la seguridad intrínseca va mucho más allá de la mera minimización del riesgo operativo. Las inversiones en ciberresiliencia se traducen en un entorno mejor y más positivo para la productividad y la innovación. Cuando los empleados pueden trabajar en cualquier lugar de forma segura y con confianza, pueden esforzarse al máximo en la innovación.

[Leer el eBook](#)

[Cómo puede ayudarle Dell Technologies](#)

Acerca de Dell Technologies

La tecnología nunca ha sido más importante que en la era actual basada en los datos y Dell considera que es un motor de progreso enormemente positivo. Tenemos el compromiso de ayudar a proteger el papel de la tecnología en el progreso humano ayudándole a planificar, prepararse y protegerse frente a ataques para que pueda desarrollar la innovación con confianza.



Acerca de Intel

En las instalaciones, en la cloud pública o en el perímetro, Dell Technologies e Intel trabajan conjuntamente para garantizar un rendimiento óptimo en una gran variedad de cargas de trabajo. La cartera centrada en los datos de Intel se basa en décadas de optimización de aplicaciones, diseñadas para ayudar a su negocio a moverse más rápido, almacenar más y procesarlo todo desde el perímetro hasta la cloud.



Acerca de VMware

Juntos, VMware y Dell aportan un valor exclusivo a nuestros clientes compartidos. Nuestras soluciones y plataformas integradas, combinadas con una escala global y la estrecha colaboración con nuestros clientes, aceleran el viaje hacia la transformación digital. El innovador software de Anywhere Workspace, de múltiples clouds y de modernización de aplicaciones de VMware funciona conjuntamente con la amplia cartera de tecnología informática de Dell Technologies, que abarca desde puntos finales hasta la cloud para ayudar a los clientes a lograr operaciones seguras y coherentes y acelerar el tiempo de rentabilización.



Todos los nombres, logotipos, marcas y marcas comerciales de los productos son propiedad de sus respectivos titulares. La información incluida en esta publicación se ha obtenido mediante fuentes que TechTarget, Inc. considera fiables, pero no está garantizada por TechTarget, Inc. La presente publicación puede contener opiniones de TechTarget, Inc., que están sujetas a cambios. Esta publicación puede incluir previsiones, proyecciones y otras declaraciones de carácter predictivo que representen los supuestos y las expectativas de TechTarget, Inc. a partir de información disponible actualmente. Estos pronósticos se basan en tendencias del sector, por lo que tienen un componente de variabilidad e incertidumbre. En consecuencia, TechTarget, Inc. no ofrece garantías sobre la exactitud de las previsiones, las proyecciones o las afirmaciones predictivas específicas incluidas en el presente documento.

Igualmente, esta publicación está bajo derechos de autor de TechTarget, Inc. Cualquier reproducción o redistribución de esta publicación, en su totalidad o en parte, ya sea en formato de copia impresa, por Internet o a personas no autorizadas para recibirla, sin el expreso consentimiento de Tech Target, Inc., constituye una violación a la ley de copyright de los EE. UU. y quedará sujeta a una demanda por daños civiles y, si corresponde, a acciones penales. En caso de duda, póngase en contacto con el servicio de relaciones con los clientes en cr@esg-global.com.



Enterprise Strategy Group es una empresa de análisis de tecnología, investigación y estrategia integrada que proporciona inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad internacional de TI.



www.esg-global.com



contact@esg-global.com



508.482.0188