DELL Technologies

# Ciberseguridad avanzada y madurez de la resiliencia

## La madurez en ciberseguridad es una palanca estratégica para cualquier empresa moderna

El panorama actual de amenazas cibernéticas es más dinámico y exigente que nunca, con ataques impulsados por IA que aumentan en frecuencia, velocidad y sofisticación. Las organizaciones ya no pueden confiar en defensas fragmentadas ni en actualizaciones incrementales.

Como líder empresarial, debe operar como si una vulneración fuera inevitable, si no inminente. En Dell Technologies ayudamos a nuestros clientes a incrementar su nivel de madurez en seguridad, es decir, el grado de confianza con el que pueden operar su negocio frente al riesgo cibernético. Lo hacemos mediante el fortalecimiento de un enfoque integral y por capas de ciberseguridad y resiliencia, estructurado en torno a tres ámbitos de actuación clave.

Las empresas deben contar con capacidades para:

- **Reducir la superficie de ataque**
- **Detectar ciberamenazas y responder ante ellas**
- **Recuperación de ciberataques**

Una ciberseguridad eficaz comienza con una evaluación honesta de su postura de seguridad actual y de su nivel de madurez. Esa claridad le permite priorizar las mejoras adecuadas e invertir en un futuro más seguro.

# Reduzca la superficie de ataque

La superficie de ataque de una organización es dinámica y evoluciona con rapidez, y la IA introduce nuevos vectores de ataque. Junto con el trabajo remoto y los sistemas heredados, estos factores amplían la superficie de ataque y crean más puntos de entrada para los actores maliciosos. Esto convierte la reducción de la superficie de ataque en una necesidad estratégica para disminuir el riesgo, cumplir las obligaciones normativas, proteger la resiliencia de la organización y generar una base sólida de confianza.

# Ciberseguridad avanzada y madurez de la resiliencia

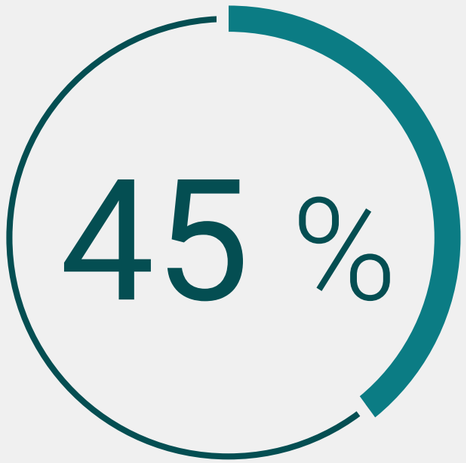
Reducir la superficie de ataque le permite disminuir el riesgo global al minimizar los puntos de entrada que los atacantes pueden explotar. Esto refuerza su nivel de madurez en seguridad y facilita el cumplimiento normativo. El resultado es una mayor resiliencia, menores costes al evitar incidentes y la capacidad de avanzar con mayor rapidez, innovar con mayor libertad y acceder a nuevos mercados con la confianza de que la seguridad está integrada desde el inicio. Todo comienza con la adopción de los principios de confianza cero (nunca confíe, siempre verifique) y con la aplicación del principio de mínimo privilegio en usuarios, dispositivos y aplicaciones.

En Dell Technologies adoptamos una mentalidad de "seguridad desde el diseño". La ciberseguridad está integrada en todo lo que hacemos, desde nuestra cadena de suministro global segura hasta las protecciones incorporadas en nuestros productos principales. Estas protecciones comienzan en el nivel de hardware para contribuir a que los dispositivos inicien y ejecuten únicamente software de confianza. Alineamos nuestras soluciones con los principios de confianza cero para ayudarle a eliminar vulnerabilidades antes de que los atacantes puedan explotarlas. Nuestros AI PC más seguros del mundo,[1] por ejemplo, proporcionan defensas fundamentales para el entorno de trabajo moderno.

Reducir la superficie de ataque incrementa su madurez en seguridad al eliminar la incertidumbre: menos elementos desconocidos, menos puntos de entrada y menos sorpresas.

**Resultados clave para el cliente:**

- **Minimización de las vulnerabilidades:** al reforzar de forma proactiva los puntos finales, la infraestructura y las aplicaciones, puede reducir de manera significativa las oportunidades de los atacantes.
- **Gestión de seguridad simplificada:** menos activos expuestos implican menos controles que gestionar, lo que se traduce en un estado de seguridad más ágil y eficiente.
- **Base más sólida para la innovación:** con puntos finales de confianza y datos protegidos, puede adoptar nuevas tecnologías como la IA y la computación en el perímetro con mayor seguridad.




Las organizaciones que se centran en reducir su superficie de ataque logran una disminución del 45 % en el riesgo de brechas de seguridad al gestionar exposiciones externas.[2]

# Detectar y responder a ciberamenazas

En el ámbito de la ciberseguridad, la velocidad y la inteligencia van de la mano. Una detección y respuesta eficaces le permiten identificar y contener las amenazas con rapidez, reducir el tiempo de permanencia y limitar el impacto de un ataque. El resultado son menores costes, menos tiempo de inactividad y una mayor confianza operativa en la capacidad de su negocio para funcionar de forma segura incluso bajo una amenaza constante.

# Ciberseguridad avanzada y madurez de la resiliencia

Sin embargo, muchas organizaciones afrontan dificultades debido a la visibilidad limitada en entornos híbridos y al volumen abrumador de alertas. En la actualidad, los atacantes permanecen dentro de las redes una media de 11 días antes de ser detectados. Para contrarrestar esta situación, necesita visibilidad en tiempo real de puntos finales, redes y sistemas mediante monitorización continua, inteligencia de amenazas y automatización.

Los socios de seguridad adecuados proporcionan conocimientos especializados en inteligencia contra amenazas y respuesta ante incidentes. Dell combina análisis avanzados, detección de amenazas basada en IA y ML, y servicios gestionados 24x7 con una base de hardware segura para identificar y contener amenazas antes de que provoquen interrupciones. Servicios opcionales como nuestro Managed Detection and Response (MDR) proporcionan experiencia en seguridad para ampliar la visibilidad y responder y mitigar amenazas con rapidez.

Las sólidas capacidades de detección y respuesta aumentan su madurez en seguridad al reducir el tiempo de permanencia y dar a los equipos la confianza necesaria para actuar con decisión cuando surgen amenazas.

**Resultados clave para el cliente:**

- **Detección más rápida y menor tiempo de permanencia:** los servicios gestionados de detección y respuesta (MDR) pueden reducir el tiempo medio de detección y respuesta entre un 25 % y un 49 %, lo que disminuye la probabilidad de que un ataque se agrave.
- **Reducción de la carga operativa:** colaborar con expertos en búsqueda proactiva de amenazas y monitorización continua traslada la carga de trabajo de los equipos internos y les permite centrarse en iniciativas estratégicas.
- **Mayor resiliencia:** capacidades maduras de detección y respuesta reducen el número de incidentes de seguridad y ayudan a evitar costes más elevados asociados a brechas de datos.

4,44 M$

El coste medio de una vulneración de datos alcanzó los 4,44 millones de dólares en 2025.[3]

# Recuperarse de un ciberataque

Cuando se produce el peor escenario, el objetivo principal consiste en restablecer las operaciones normales lo antes posible y con la mínima interrupción. Recuperarse de un ciberataque le permite restaurar rápidamente datos y sistemas limpios, reducir el impacto reputacional y tener la certeza de que la recuperación es fiable y está libre de reinfecciones.

# Ciberseguridad avanzada y madurez de la resiliencia

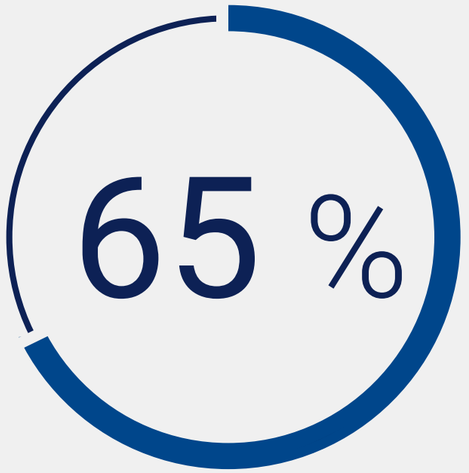
A pesar de que es fundamental construir las defensas más sólidas posibles, también es necesario planificar como si un ataque fuera inevitable. Disponer de un plan integral de recuperación y de las capacidades necesarias resulta fundamental. Esto incluye mantener copias de seguridad limpias e inmutables de los datos críticos en un vault de recuperación aislado y utilizar entornos de sala blanca para validar que los sistemas restaurados estén libres de malware antes de volver a ponerlos en funcionamiento.

Dell incorpora capacidades de recuperación en nuestras ofertas de productos, y lograr que las empresas vuelvan a funcionar con normalidad es nuestra primera prioridad cuando se producen incidentes. Soluciones como PowerProtect Cyber Recovery Vault aíslan y protegen copias limpias de datos críticos para facilitar una recuperación rápida, limitar las pérdidas y restar capacidad de presión a los atacantes de ransomware. Esta arquitectura le ayuda a restablecer con rapidez las cargas de trabajo críticas y a operar con mayor confianza.

La recuperación es, con frecuencia, el momento en el que se pone realmente a prueba la madurez en seguridad, cuando la confianza depende de la rapidez y la limpieza con las que el negocio puede volver a la normalidad.

**Resultados clave para el cliente:**

- **Reducción del impacto en el negocio:** las organizaciones con un plan de respuesta ante incidentes bien ensayado pueden reducir los costes derivados de una brecha en aproximadamente un 61 %.
- **Reanudación más rápida de las operaciones:** priorizar el rápido restablecimiento de la actividad, y no solo la eliminación de la amenaza permite recuperar la operatividad con una interrupción y un coste mínimos.
- **Mayor integridad de los datos:** aislar los datos críticos, utilizar copias inmutables y validar la integridad antes de la restauración refuerza la confianza en el proceso de recuperación.




de las organizaciones admitieron que les costaría recuperarse de un ciberataque y, al mismo tiempo, cumplir sus acuerdos de nivel de servicio[4]

# Refuerce su estado de seguridad mediante asociaciones estratégicas

Los socios con experiencia resultan esenciales para desenvolverse en el actual panorama de ciberseguridad, dinámico y complejo. Las ciberamenazas son cada vez más sofisticadas y frecuentes, lo que hace casi imposible que una única organización mantenga por sí sola la experiencia, los recursos y la tecnología necesarios para anticiparse a ellas. Al colaborar con líderes en seguridad como Dell, las empresas acceden a competencias especializadas, tecnologías avanzadas y una red de socios de confianza. Estas alianzas proporcionan el respaldo y la experiencia necesarios para detectar, prevenir y responder a las amenazas de forma eficaz, y garantizan que las organizaciones permanezcan protegidas en un entorno digital en constante evolución.

Con el enfoque adecuado en estos tres ámbitos de actuación, las organizaciones incrementan su madurez en seguridad y adquieren la confianza necesaria para operar, innovar y crecer pese a la presión cibernética constante. Dell reúne infraestructura de confianza, un entorno de trabajo seguro, servicios avanzados y un ecosistema de socios para reforzar la seguridad, la capacidad de adaptación y la resiliencia de su organización frente a los desafíos futuros.

**Explorar las soluciones de seguridad**

## Preguntas frecuentes

**1. ¿Por qué debe la ciberseguridad ser una prioridad estratégica para mi empresa?**
*La ciberseguridad es mucho más que un mecanismo de protección; es la base que permite a una empresa innovar y crecer mientras afronta un entorno de amenazas cada vez más exigente. Un estado de seguridad sólido no se limita a la defensa, sino que actúa como facilitador. Las empresas con marcos de ciberseguridad maduros avanzan con mayor rapidez, innovan con mayor libertad y acceden a nuevos mercados con mayor confianza. Además, están mejor preparadas para gestionar cambios normativos, responder a las demandas de los clientes y hacer frente a la presión competitiva.*

**2. ¿Cómo podemos equilibrar la necesidad de una seguridad estricta con la libertad para innovar?**
*No debería tener que elegir entre seguridad e innovación. Creemos que una seguridad robusta impulsa la innovación. Cuando cuenta con una base de "seguridad desde el diseño", en la que la protección está integrada desde el inicio en dispositivos, infraestructura y datos, sus equipos pueden adoptar nuevas tecnologías como la IA y la computación en el perímetro con confianza.*

**3. ¿Por qué es tan crítica la seguridad de la cadena de suministro?**
*La seguridad real comienza mucho antes de pulsar el botón de encendido. A medida que crece su huella digital, también aumenta su exposición, y la confianza se convierte en la primera línea de defensa. Cada eslabón de la cadena de suministro debe estar protegido, ya que un único componente comprometido puede poner en riesgo incluso el software más avanzado. Por eso integramos la seguridad desde el origen y protegemos cada fase, desde la producción hasta la implementación. Desde la fábrica hasta sus instalaciones, su tecnología llega verificada, protegida y preparada para ofrecer el rendimiento esperado con total confianza.*

**4. ¿Cómo ayuda Dell a recuperarse tras un ciberataque?**
*Cuando se produce un incidente, minimizar el tiempo de inactividad y la interrupción del negocio resulta fundamental. La preparación es clave. PowerProtect Cyber Recovery Vault aísla una copia limpia e inmutable de sus datos más críticos, separada de forma segura del entorno principal. En caso de incidente, puede restablecer las operaciones con rapidez y confianza, sin comprometer la integridad de los datos y sin pagar un rescate.*
*Dell ofrece una amplia gama de productos y servicios diseñados para ayudarle a implementar una estrategia integral de recuperación. Esta incluye desde servicios de consultoría para definir un plan de recuperación y formación, hasta capacidades avanzadas de protección de datos que mantienen a salvo la información crítica. Dell adopta un enfoque centrado en las personas y en la tecnología, con el fin de garantizar que ambos elementos trabajen de forma coordinada para facilitar una recuperación ágil y eficaz.*

**5. ¿Puede Dell ayudar con la detección de amenazas en tiempo real?**
*Claro, sí. La velocidad es determinante a la hora de frenar una ciberamenaza. Combinamos funcionalidades de seguridad integradas con servicios avanzados como Managed Detection and Response (MDR) para supervisar su entorno las 24 horas del día, los 7 días de la semana. Mediante el uso de análisis basados en IA y ML junto con la experiencia humana, le ayudamos a identificar anomalías y amenazas potenciales de inmediato, lo que le permite responder y contener incidentes antes de que afecten a su negocio.*

## Fuentes


**[1] Según análisis internos de Dell en octubre de 2024 (Intel) y marzo de 2025 (AMD). Aplicable a PC con procesadores Intel y AMD. No todas las funciones están disponibles en todos los PC. Algunas funciones requieren compras adicionales. PC con tecnología Intel validados por Principled Technologies, julio de 2025, infografía de la anatomía de un dispositivo de confianza**

**[2] Forrester Consulting, "The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight," octubre de 2024.**

**[3] IBM y Ponemon Institute, "Cost of a Data Breach Report 2025: The AI Oversight Gap", 2025.**

**[4] Dell Technologies, "Impulse la madurez en ciberseguridad: La infraestructura tecnológica es el corazón de las empresas modernas", febrero de 2025.**


### Acerca de Dell Technologies

Dell Technologies (NYSE:DELL) ayuda a las organizaciones y a las personas a crear su futuro digital y a transformar su forma de trabajar, vivir y jugar. La empresa proporciona a los clientes la cartera de tecnologías y servicios más amplia e innovadora del sector para la era de la IA.



Obtenga más información en Dell.com