



¿Está preparado para un incidente cibernético disruptivo?

Los riesgos y costes asociados de los ciberataques siguen aumentando, siendo los ataques de ransomware unos de los más dañinos para las operaciones empresariales. La imposibilidad de desarrollar la actividad empresarial durante un tiempo prolongado (semanas o incluso meses) puede resultar devastadora para el éxito a largo plazo de la organización.

La recuperación es crítica y el esfuerzo necesario para volver al funcionamiento normal de la empresa es extremadamente complicado. Para restaurar los servidores y las ingentes cantidades de datos y aplicaciones, conseguir que las aplicaciones más críticas vuelvan a estar disponibles lo antes posible y cumplir con los objetivos de tiempo de recuperación (RTO), es necesario llevar a cabo un gran esfuerzo.

72 %

de las empresas declara necesitar ayuda externa para asegurarse de que cubren todos los requisitos de seguridad y riesgo del entorno de TI.⁵

Le prestamos ayuda esencial para que pueda volver a desarrollar su actividad empresarial

Servicios de recuperación y respuesta ante incidentes

Nuestro equipo de expertos en ciberseguridad certificados en el sector colaboran con usted en cada paso del camino. Gracias al respaldo de la escala que tiene la red global de Dell Technologies, podemos reaccionar rápidamente para eliminar la amenaza y restaurar la actividad empresarial rápidamente y con el menor tiempo de interrupción posible.

Las amenazas cibernéticas siguen creciendo y los efectos pueden ser devastadores

Cada **11 segundos** se produce un ataque de ciberseguridad o ransomware que logra su objetivo¹

16 días el tiempo de inactividad medio tras un ataque de ransomware²

75 % de las organizaciones se enfrentarán a uno o más ataques antes de 2025³

Más del **60 %** de las empresas han sufrido una pérdida de datos debido a la explotación de una vulnerabilidad⁴

Servicios de recuperación y respuesta ante incidentes

En Dell Technologies Services, contamos con una trayectoria demostrada en lo que se refiere a recuperar clientes que han experimentado un incidente cibernético.

**Se ha producido un incidente.
¿Cuál es el siguiente paso?**

Obtenga ayuda

Recuperación

Las operaciones se ven afectadas y podrían producirse las siguientes situaciones:

- El correo electrónico no funciona.
- No se puede acceder a los datos.
- Malware.
- La red está inactiva.
- Active Directory no está activo.
- Las transacciones no se pueden procesar.
- Se ha pedido un rescate.

Obtenga ayuda

Nuestro equipo de expertos está preparado para una respuesta inmediata. Lo único que tiene que hacer es ponerse en contacto con nosotros en: Incident.Recovery@dell.com

Equipo de recuperación y respuesta ante incidentes (IRR)

Expertos que le acompañarán en cada paso del camino.

Confíe en los expertos

Nuestro equipo dedicado de expertos en ciberseguridad certificados en el sector cuenta con un gran conocimiento y sigue los procedimientos recomendados en una amplia gama de talentos y dominios

Obtenga la ayuda que necesita, independientemente de la situación

Nuestros servicios se adaptan a sus necesidades independientemente de la situación a la que se enfrente o de los aspectos que se hayan visto afectados. Primero evaluamos su situación y después nos ponemos en contacto con los recursos adecuados para ayudarle a recuperarse rápidamente.

Qué hacemos

Tanto si acaba de producirse un ataque como si ya ha estado trabajando en la recuperación y necesita ayuda para avanzar más rápidamente, nuestros expertos están preparados para lo siguiente:

- Evaluar e implementar los recursos adecuados.
- Erradicar la amenaza y mitigar los riesgos de seguridad.
- Recuperar las aplicaciones de empresa para que vuelvan a funcionar como antes del incidente.
- Volver a implementar puestos de trabajo para que los empleados puedan volver a trabajar.
- Prestar servicios forenses de datos de expertos.
- Ayudar a mejorar la seguridad.

Obtenga ayuda

- Llámenos en cuestión de minutos u horas y solicite que un equipo vaya a sus instalaciones en menos de 48 horas.
- Consiga más de 100 recursos con múltiples flujos de trabajo en distintas ubicaciones e idiomas, con flexibilidad para ajustarlos según sea necesario.
- Proporcione expertos en ciberseguridad certificados en el sector, la mayoría con más de 10 años de experiencia.
- Ofrezca experiencia y conocimientos sobre la infraestructura y los dispositivos de punto final tanto de Dell como de otras marcas.
- Aporte conocimiento y experiencia en el periféricos, cloud, aspectos legales y seguros, entre otros.
- Alcance global a más de 170 mercados
- Aproveche las innovadoras soluciones de pago que le permiten adaptar y escalar el coste de las soluciones informáticas según el consumo de tecnología y la disponibilidad presupuestaria.**

Recuperación

- Elimine el origen de las amenazas.
- Recupere el funcionamiento normal de su empresa rápidamente.
- Aumente el personal de TI existente debido al aumento de la carga de trabajo.
- Reconstruya un entorno de red reforzado.
- Mejore el estado de seguridad mediante el desarrollo y la implementación de una estrategia de seguridad para evitar ciberataques repetidos.
- Forme y comparta los procedimientos recomendados.

Para obtener más información, visite Delltechnologies.com/incident-response-and-recovery

** Soluciones de pago proporcionadas a clientes comerciales cualificados a través de Dell Financial Services (DFS) o a través de empresas del grupo Dell Technologies o a través de socios comerciales autorizados de Dell (junto con DFS "Dell"). Es posible que las ofertas varíen o no estén disponibles en función del país. Las ofertas pueden modificarse sin previo aviso y están sujetas a la disponibilidad de los productos, a la elegibilidad, a la aprobación del crédito y a la ejecución de la documentación proporcionada y aceptada por Dell o los socios comerciales autorizados de Dell. En España, los servicios son proporcionados por la sucursal de Dell Bank International d.a.c en España y en el resto de la UE por Dell Bank International d.a.c, bajo el nombre comercial Dell Financial Services, que está regulado por el Banco Central de Irlanda. Dell Technologies, DellEMC y los logotipos de Dell son marcas comerciales de Dell Inc.

¹ Estimado para 2021, Cybersecurity Ventures: <https://cybersecurityventures.com>

² Por qué el ransomware cuesta a las empresas mucho más que dinero; Forbes, 30 de abril de 2021, <https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6>

³ Detect, Protect, Recover: How Modern Backup Applications can protect you from ransomware (Detección, protección, recuperación: cómo las aplicaciones de copia de seguridad modernas pueden protegerle del ransomware), Nik Simpson, Gartner, 6 de enero de 2021, <https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb>

⁴ Informe acerca del liderazgo intelectual realizado por Forrester Consulting por encargo de Dell, "BIOS Security – The Next Frontier for Endpoint Protection", junio de 2019

⁵ Estudio de Forrester Consulting encargado por Dell Technologies, diciembre de 2020.