Conocimiento y recursos para recuperarse rápidamente de un ciberataque

Confíe en que estará bien preparado ante un incidente cibernético disruptivo

Dell Incident Recovery Retainer Service

Los riesgos y los costes que conllevan los ciberataques no cesan de aumentar. Si pierde la capacidad de desarrollar su actividad comercial, el rendimiento financiero, las relaciones con los clientes, el cumplimiento de la normativa y la reputación de la empresa se verían afectados.

Cuando se produce un ataque, la velocidad de respuesta es crucial para poder recuperarse correctamente. Sin embargo, las tareas para volver a la actividad normal pueden ser extremadamente complejas. Además de lidiar con el incidente, es necesario restablecer los entornos de TI y existen cantidades masivas de datos que deben restaurarse para volver a conectar las aplicaciones críticas con un retraso mínimo.

75 %
de las organizaciones se enfrentarán a uno o más ataques antes de 2025.[1]

97 %
de tasa de éxito que exhibe Dell en la recuperación de las operaciones de clientes que han sufrido un ciberataque.[2]

16 días
es el tiempo de inactividad medio tras un ataque con programas de secuestro.[3]

Muchos equipos de TI no disponen de la capacidad suficiente ni la combinación de habilidades necesarias para recuperarse de un ciberataque. Con Dell Incident Recovery Retainer Service, dispondrá de un equipo de expertos certificados en el sector de la ciberseguridad y las infraestructuras que trabajarán a su lado para restaurar su entorno. El servicio incluye 120 o 240 horas de asistencia para la recuperación, lo que significa que no habrá que esperar a la autorización del pedido, ya que nuestro equipo empezará a trabajar en la recuperación de inmediato.

Evaluación del grado de preparación para la recuperación. Cuando se inicia el servicio, creemos que resulta importante comprender la estrategia de recuperación y restauración actual de la organización. Nuestro experimentado equipo revisará los planes de recuperación, la red y la infraestructura, así como los procesos de copia de seguridad existentes, entre otros factores. El equipo prepara un informe de resumen de la evaluación y la planificación con el fin de trazar un roadmap para mejorar su nivel de preparación ante incidentes y la forma de abordar la recuperación.

Principales beneficios

- En caso de incidente:
  - Obtendrá una respuesta rápida por parte de profesionales de Dell altamente cualificados y experimentados en ciberseguridad
  - Nuestro equipo evaluará rápidamente su situación y determinará el mejor plan de acción para minimizar las interrupciones comerciales de la actividad empresarial
  - La amenaza se eliminará y la vulnerabilidad que aprovechó el atacante quedará cerrada[4]
- El modelo de este servicio ofrece 120 o 240 horas anuales de asistencia para la recuperación
- El equipo de ciberseguridad de Dell Technologies aporta diversas experiencias, habilidades y herramientas a cada situación única de los clientes
- Evaluación inicial del nivel de preparación para la recuperación de las funciones y la cobertura de recuperación existentes, incluido el informe de resumen para establecer las prioridades de los aspectos a mejorar
- El proceso de recuperación es más eficiente dado que el equipo de Dell se familiariza con su entorno a través de la evaluación inicial

Funciones principales

120 o 240 horas al año para actividades de recuperación ante incidentes

- Prestación remota (en algunas regiones, el servicio in situ está disponible con sujeción a tasas adicionales)
- El gestor de proyecto supervisa las actividades
- Evaluación del incidente y la situación
- Asignación e implementación de recursos
- Análisis forense: digital, malware y datos
- Eliminación de las amenazas
- Saneamiento, recuperación y conservación de datos
- Restablecimiento del entorno y las aplicaciones

Evaluación de las funciones de recuperación ante incidentes

- Se desarrolla al inicio de la contratación
- Identificación de la red, la infraestructura y los centros del cliente para estar preparado con el fin de poder dar una respuesta en caso de incidentes de ciberseguridad
- Revisión del plan de recuperación ante incidentes y las funciones de copia de seguridad y restauración de datos
- Dell prepara un informe de resumen que incluye recomendaciones para mejorar el nivel de preparación y la forma de abordar la recuperación

Niveles de servicio:

- Se programa una reunión de inicio del servicio con el cliente en 2 horas tras la solicitud inicial por parte del cliente (tiempo medio de reacción)
- La respuesta remota comienza en las 6 horas posteriores a la reunión de inicio del servicio (tiempo medio de respuesta)
- Si se ha acordado que la respuesta se realice in situ, se iniciará en las 24 horas posteriores a la reunión de inicio del servicio (tiempo medio de respuesta)

Las horas transcurridas y el saldo restante se revisarán con el cliente cada trimestre

- En caso de que las horas para la recuperación y la restauración no se consuman por completo, las horas restantes podrán emplearse en asesoramiento por parte de expertos para la planificación de la recuperación ante incidentes, mejoras en ciberseguridad y en áreas relacionadas

Prepárese

No hay forma de saber exactamente cuándo su organización sufrirá un incidente cibernético grave. Asegúrese de estar preparado con Dell Incident Recovery Retainer Service. Podrá estar tranquilo porque contará con el apoyo de profesionales en ciberseguridad altamente cualificados y experimentados que le atenderán de inmediato y trabajarán para eliminar las amenazas y restablecer sus operaciones críticas.

Póngase en contacto con su representante de ventas hoy mismo

[1] "Detect, Protect, Recover: How modern backup applications can protect you from ransomware", Nik Simpson, Gartner, 6 de enero de 2021. ID de documento de Gartner: G00733304. https://www.gartner.com/en/documents/3995229

[2] Información basada en análisis de Dell sobre las solicitudes de servicio que tuvieron lugar entre junio de 2019 y julio de 2021 en Norteamérica.

[3] "Why Ransomware Costs Businesses Much More than Money", 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

[4] Si se requieren más de las 120 o 240 horas anuales incluidas de trabajo de recuperación, se pueden adquirir horas adicionales.