LIBRO ELECTRÓNICO

# Ciberresiliencia: protege tus datos desde dentro hacia fuera

NetApp

# Información general



# Viaje al centro de la organización tecnológica

Es el día de hacer la compra. Coges las bolsas desechables, las llaves y te tomas una enorme píldora plateada, la píldora de resistencia del conductor, antes de salir por la puerta.

Ahora puedes conducir sabiendo que tu cuerpo tiene la habilidad sobrehumana de enfrentarse a cualquier riesgo de camino al mercado.

Si pudiéramos tomarnos un brebaje mágico de resistencia, construir casas con ladrillos que expulsen a los intrusos o comprar joyas que salgan volando de las manos de un ladrón, apenas nos molestaríamos en usar cinturones de seguridad, cerraduras y alarmas.

## Un nuevo enfoque de la ciberseguridad

Puede que no existan estas protecciones mágicas en el mundo real, pero comienzan a emerger en el virtual. Convergen con los dispositivos de protección existentes. Durante las últimas décadas, el mundo tecnológico ha usado el método de «cinturones y alarmas» porque eso es lo que había.

Hoy, existe un método más inteligente: la ***resiliencia cibernética***.

La resiliencia cibernética combina la protección de datos con la seguridad de datos para que las organizaciones puedan recuperarse de un ciberataque. Incluso si un intruso se infiltra en el perímetro o alguien realiza una acción malintencionada desde dentro, los datos permanecen a salvo, porque cuentan con una protección incorporada en lugar de seguridad en torno a ellos desarrollada a última hora.

## Su importancia

Las medidas de ciberseguridad centradas únicamente en la protección contra amenazas externas no les siguen el ritmo a las tácticas ilegales en constante evolución. Hoy:

- La mayoría de las estrategias de seguridad pasan por detener al enemigo en la puerta fortificando el perímetro.
- Las empresas no defienden solo una puerta. Son responsables de cientos de ellas debido a la proliferación de los puntos de conexión, las políticas que permiten utilizar dispositivos personales y el auge del teletrabajo.
- Ahora es más fácil que nunca que los delincuentes pongan en peligro organizaciones que ya de por sí están demasiado ocupadas para supervisar a fondo los complejos entornos de red.

Además, muchas organizaciones olvidan que el objetivo no es evitar las intrusiones. El objetivo principal es proteger lo más valioso: **tus datos**.

# **Resiliencia cibernética** *frase nominal*

re-si-lien-cia·ci-ber-né-ti-ca

La capacidad de anticiparse, resistir, recuperarse y adaptarse a condiciones adversas, esfuerzos, ataques o riesgos que usan o vienen derivados de los recursos cibernéticos[1]

# ¿Tu estrategia de resiliencia cibernética empieza por lo más importante?

## Con amenazas por todas partes, ¿por dónde empezar?

Empieza por poner los datos en el centro de la seguridad y protección. Que sean parte esencial de tu plan de resiliencia cibernética. En el panorama de amenazas de hoy en día:

- **Con un aumento del 62 % de ransomware en el mundo**[2] y con un 3,4 % más de familias de ransomware,[3] los atacantes son cada vez mejores secuestrando datos.
- **Aproximadamente un tercio de las organizaciones tienen que pagar** para recuperar sus datos cifrados tras un ataque de ransomware.[4]
- **El coste medio del rescate de un ataque de ransomware en 2021 era de 1,85 millones de dólares americanos**. En 2020, la cifra era de 768 106 dólares americanos.[5]
- **Cada vez hay más ataques de ransomware de doble extorsión**, lo que significa que las organizaciones no solo corren el riesgo de perder sus datos, sino también de que se hagan públicos.[6]

Los riesgos nunca habían sido tan altos y los ataques de ransomware se han convertido en una realidad para la computación moderna.

Pero, ¿tienes que vivir con miedo al próximo ataque de ransomware? No. Di adiós al miedo al ransomware y **activa la resiliencia cibernética** con una estrategia de ciberseguridad centrada en los datos.

Este enfoque implica empezar lo más cerca posible de los datos, en lugar de hacerlo en el perímetro.

# Traza el camino hacia una mayor resiliencia cibernética

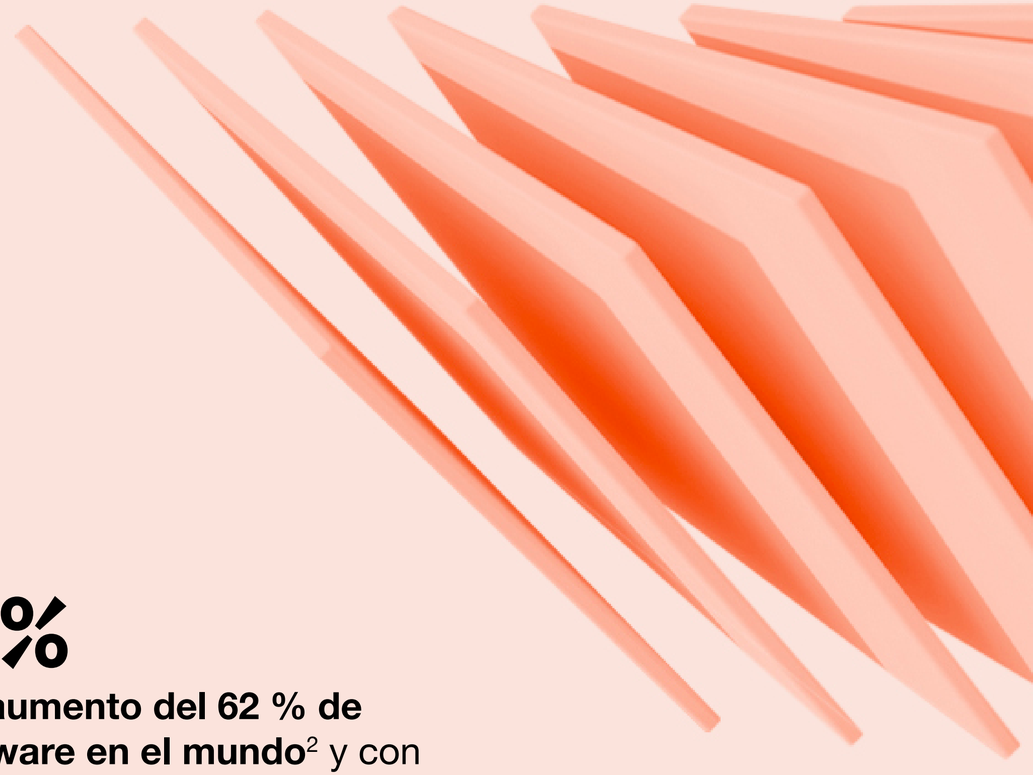
Si vas a viajar al centro de tu organización de TI para proteger los datos, hay que hacer un esfuerzo. Afortunadamente, otros ya se han aventurado y han dejado algunas guías útiles:

**Identificación** **Protección** **Detección**

**Respuesta** **Recuperación**

Incluso con estos indicadores como ayuda, la creación de un plan integral de resiliencia cibernética sigue siendo difícil y costosa. Tu equipo tiene que hacer malabarismos con recursos limitados, cubrir lagunas de conocimientos, incorporar requisitos normativos y compaginar su atención con otras prioridades.[7] La resiliencia cibernética puede resultar agotadora (y olvidarse) rápidamente.

**Aquí explicamos cómo enfrentarse a cada paso.**



**62 %**

Con un **aumento del 62 % de ransomware en el mundo**[2] y con un **3,4 % más de familias de ransomware**,[3] los atacantes son cada vez mejores secuestrando datos.

# Identificación:
## Analiza tu entorno

Identifica qué necesita protección y clasifica cada elemento según su importancia. Deberías hacerte preguntas como estas:

P:

**¿Sabes dónde residen tus datos y qué tipos de datos hay en tu entorno?**

**Para cada tipo de datos, ¿es confidencial? ¿Quién tiene permisos de acceso?**

**¿Qué sistemas son esenciales para mantener las operaciones empresariales?**

**¿Qué papel tiene cada tecnología en tus operaciones empresariales y cómo la podría explotar un actor malintencionado?**

**¿Se documentan los flujos de información?**

**¿Qué relación tienen las funciones y responsabilidades con las actividades de seguridad cibernética asignadas?**

**¿Cuál es tu plan de identificación de amenazas y gestión de riesgos?**[7]

**¿Cuáles son tus soluciones de seguridad y protección de datos actuales?**

En otras palabras, tendrás que evaluar la actual protección y seguridad de tus datos. También tendrás que clasificar los distintos tipos de datos, determinar dónde se encuentran y evaluar sus permisos.

### Desafíos asociados con la fase de identificación

La fase de identificación requiere mucho tiempo. Los responsables tecnológicos ya tienen un montón de tareas diarias de gestión de infraestructuras y datos. Solo el inventario de la infraestructura tecnológica, especialmente sin herramientas de automatización, puede requerir una cantidad significativa de tiempo.

Si este proceso de inventario no se lleva a cabo con un plan específico o con protocolos de clasificación estandarizados, puede crear un conjunto de datos aún más confuso que a los equipos les cueste descifrar y aprovechar.

# Protección:
# Prepara tus defensas

En la fase de protección, prepara tus defensas.

Cifra los datos, realiza copias de seguridad periódicas, asegura el control de acceso, implementa defensas perimetrales, actualiza los sistemas operativos y las aplicaciones vulnerables, y forma a los usuarios sobre las mejores prácticas de ciberseguridad.[7]

Esta etapa implica bloquear a los usuarios malintencionados, poner en cuarentena los datos potencialmente dañinos, impedir que se escriban datos adicionales en un disco, crear copias granulares inmutables que frustren la infección y evitar el borrado de datos con copias de seguridad indelebles.

## Desafíos asociados a la etapa de protección

La etapa de protección revela algunos de los cambios más recientes en la estrategia de ciberseguridad. Aunque las empresas llevan décadas utilizando cortafuegos y herramientas de intrusión de red para proteger sus entornos informáticos, la nueva realidad de cantidades masivas de datos ha complicado estas estrategias. Los equipos tecnológicos deben responder a preguntas difíciles como las siguientes:

- ¿Cómo puedes cifrar grandes cantidades de datos que se generan más rápido de lo que se pueden registrar?
- ¿Cómo puedes garantizar el control de acceso sin comprometer gravemente la experiencia del usuario (lo que podría llevar a niveles de productividad más bajos o a soluciones no seguras)?
- ¿Cómo puedes tener claro que has cubierto todo, dada la cantidad de puntos ciegos que has descubierto?
- ¿Qué pruebas realizas con frecuencia en tus tecnologías de protección de datos para garantizar que, en caso de amenaza, puedas recuperar los datos con éxito?

# Detección:
# Ve un paso por delante

Más vale prevenir que curar. Pon en marcha sistemas que identifiquen la actividad sospechosa antes de que se convierta en una amenaza real, como los siguientes:

- Procesos de detección actualizados
- Registros supervisados regularmente para poder detectar y abordar la actividad anómala
- Un conocimiento exhaustivo de los flujos de datos habituales, para poder detectar actividades inusuales que puedan indicar un robo de datos
- La capacidad no solo de detectar, sino también de calcular el impacto (o «radio de explosión») de una filtración[7]

En otras palabras, tienes que controlar el comportamiento de los usuarios para detectar actividades sospechosas y detectar anomalías en el comportamiento de los datos.

## Desafíos asociados a la etapa de detección

**Gestionar el ruido en las alertas:** posiblemente, el mayor reto de la etapa de detección es la cantidad de ruido que las empresas deben filtrar. Los equipos de ciberseguridad y los centros de operaciones de seguridad (SOC) se ven abrumados por las alertas de amenazas, que a menudo tienen que analizar manualmente.

**Automatizar la clasificación de amenazas**: necesitan una forma de investigar y eliminar automáticamente las alarmas falsas y de baja prioridad, para poder dedicar su atención a las más complicadas.

**Aumentar la velocidad de detección**: los equipos de ciberseguridad también necesitan una forma de detectar estas amenazas más rápidamente, para poder responder antes de que se produzcan daños graves. En concreto, necesitan una notificación inmediata de los accesos no autorizados con credenciales comprometidas antes de que un atacante pueda cifrar una cantidad significativa de datos.

# Respuesta:
# Aprende cómo actuar ante una crisis

Las amenazas evolucionan al mismo tiempo que las medidas de seguridad. Por ello, es importante poner a prueba tus planes continuamente en tres pasos:

**1**

Todos los miembros del equipo deben conocer sus responsabilidades, tanto las prácticas recomendadas generales de ciberseguridad como sus funciones específicas en caso de emergencia.

**2**

Actualiza los planes a medida que evolucionan las amenazas y se aprenden las lecciones tras los ataques.

**3**

Comparte todas las actualizaciones del plan con otras partes interesadas, tanto internas como externas, para que haya una respuesta cohesionada si se produce un ataque.[7]

## Desafíos asociados a la etapa de respuesta

Para acertar en la etapa de respuesta, es necesario tener una visión general de tus sistemas, de modo que puedas evaluar dónde están tus datos, controlar qué tipo de actividad ocurre en el entorno y actualizar los planes en consecuencia.

De nuevo, esta actividad les lleva mucho tiempo a las organizaciones, que ya están ocupadas con sus necesidades diarias de infraestructura y gestión de datos.

Lo cierto es que cualquier respuesta eficaz debe ser más rápida que el tiempo que se tarda en ejecutar manualmente un plan, por muy preparado que se esté. Los equipos de ciberseguridad necesitan herramientas automatizadas que sigan pasos predeterminados (como tomar un snapshot de los datos) en cuanto el sistema detecte una actividad sospechosa.

# Recuperación:
# Vuelve a la normalidad con rapidez

Si un ciberataque interrumpe las operaciones de la empresa, tienes que poder retomarlas rápidamente. Es esencial saber lo siguiente:

- ¿Qué información habrá que compartir?
- ¿Quién necesitará acceso a esa información?
- ¿Cómo te asegurarás de que las partes interesadas reciban la información que necesitan en el momento oportuno?
- ¿Cómo comunicarás la vulneración al público para informar de la información que se haya podido poner en riesgo?
- ¿Qué pasos debes seguir para comunicarte con los organismos reguladores?

En la fase de recuperación, debes reducir el tiempo de inactividad y restaurar los datos rápido, volver a poner en línea las aplicaciones no comprometidas y aplicar técnicas forenses inteligentes para identificar el origen de la amenaza.

## Desafíos asociados a la etapa de recuperación

Tras un ataque, puede llevar un tiempo precioso identificar qué partes se han visto comprometidas y en qué medida. Pero necesitarás obtener esta información rápidamente si vas a gestionar tanto la respuesta interna como la óptica externa.[7]

Estas cinco partes de un plan de resiliencia cibernética (Identificación, Protección, Detección, Respuesta y Recuperación) están respaldadas por la solución de resiliencia cibernética de NetApp®. Pero muchas empresas han invertido en un mosaico de herramientas de ciberseguridad que puede hacer que la idea de cambiar de proveedor resulte agobiante.

Con NetApp, el cambio no será agobiante. Puedes introducir una solución contra el ransomware que sirva como solución completa o como complemento a tus actuales inversiones.

# Construye un modelo de resiliencia cibernética desde dentro

Fijémonos en la construcción de un enfoque moderno para la resiliencia cibernética de tu empresa que incluya las soluciones para los desafíos habituales destacados anteriormente. Las soluciones de resiliencia cibernética de NetApp se enfrentan a estos desafíos desde dentro, con soluciones de seguridad y protección diseñadas centrándose en tus datos.

La cartera de soluciones de NetApp incluye gestión de datos potente y robusta, datos inteligentes y supervisión de usuarios y servicios profesionales que ayudan a las organizaciones en cualquier fase de su preparación y gestión.

Cuando los datos se convierten en tu principal objetivo, es más fácil abordar las necesidades de resiliencia cibernética. El primer paso es comprender tu estado actual respondiendo las siguientes preguntas.

**Más vale prevenir que curar. Pon en marcha sistemas que identifiquen la actividad sospechosa antes de que se convierta en una amenaza real, como los siguientes:**

- ¿Dónde se almacenan mis datos? ¿En el cloud? ¿De manera local? ¿En el perímetro? ¿En varios sitios a la vez?
- ¿Qué tipo de datos tengo?
- ¿Qué tipo de permisos tienen mis datos?
- ¿Cómo puedo identificar y bloquear rápidamente la actividad maliciosa?
- ¿Cómo puedo asegurarme de que todos mis datos están a salvo mientras determino el alcance de un ataque?
- ¿Cómo puedo hacer que mis datos y aplicaciones vuelvan a estar en línea, en cuestión de minutos, si se produce un ataque?
- ¿Cómo puedo investigar el origen de una amenaza para tener suficiente información con la que evitar futuros intentos similares?
- ¿Cómo puedo crear una protección directamente dentro o alrededor de mis datos para que puedan «autoprotegerse» rápidamente, mientras identificamos y abordamos una amenaza? ¿Cómo puedo controlar el comportamiento de los usuarios para detectar actividades sospechosas en toda mi red?

Al responder a todas estas preguntas, crearás el esquema de un plan de resiliencia cibernética centrado en los datos que puede ayudar a tu empresa a preparase para los ataques de ransomware.

Si hay demasiadas respuestas "lo desconozco" como para sentirte cómodo servicios profesionales ofrece una solución que no solo te da respuestas, sino que proporciona las herramientas que necesitas para ejecutar tu nuevo plan de protección y recuperación contra el ransomware.

# Un plan de resiliencia cibernética en acción con NetApp

NetApp ofrece una cartera de soluciones diseñadas para cumplir las necesidades tecnológicas y de los equipos de seguridad para proteger mejor los datos. Nuestros servicios de datos se construyen por capas en una base de software de almacenamiento ONTAP®, con el objetivo de mejorar la visibilidad, detectar amenazas y automatizar la respuesta y la recuperación.

Sigue leyendo para descubrir cómo NetApp, junto con un plan de resiliencia cibernética basado en las respuestas a las anteriores preguntas, puede ayudar a tu equipo durante un ataque de ransomware.

«Hace poco sufrimos un incidente de ransomware y, al ver las capacidades de detección de ransomware que ofrece Cloud Insights, nos convenció».

Director de TI de una empresa de transporte

## Identificación

Tu equipo necesita saber qué tipo de datos tienes, si son confidenciales y dónde están ubicados para poder planificar mejor qué se protegerá y cómo. Cloud Data Sense de NetApp, una solución SaaS, usa algoritmos de inteligencia artificial para la detección, asignación y clasificación de datos para proporcionar esta información.

Por su parte, Cloud Insights de NetApp, que proporciona visibilidad de la infraestructura del cloud híbrido, permite a tu equipo supervisar y proteger todo el entorno. Y eso es algo bueno, porque tus defensas están a punto de ser puestas a prueba.

## Protección

Una mañana, tu equipo de TI en la sede en Nueva York llega al trabajo y se entera de que alguien en la oficina de Londres ha hecho clic en un enlace de correo electrónico malicioso.

Aunque no había nadie cerca para supervisar físicamente este ataque, FPolicy® de NetApp, que forma parte del software de gestión de datos ONTAP de NetApp, utilizó su protección de datos Zero-Trust para bloquear las extensiones de archivos maliciosos conocidos.

Sin embargo, los hackers persisten. Utilizan una cuenta de usuario comprometida para infectar archivos mediante un exploit de malware de día cero. Más malware se introduce en varias cuentas de usuario comprometidas para cifrar los datos lentamente, con la esperanza de evitar la detección.

## Detección y respuesta

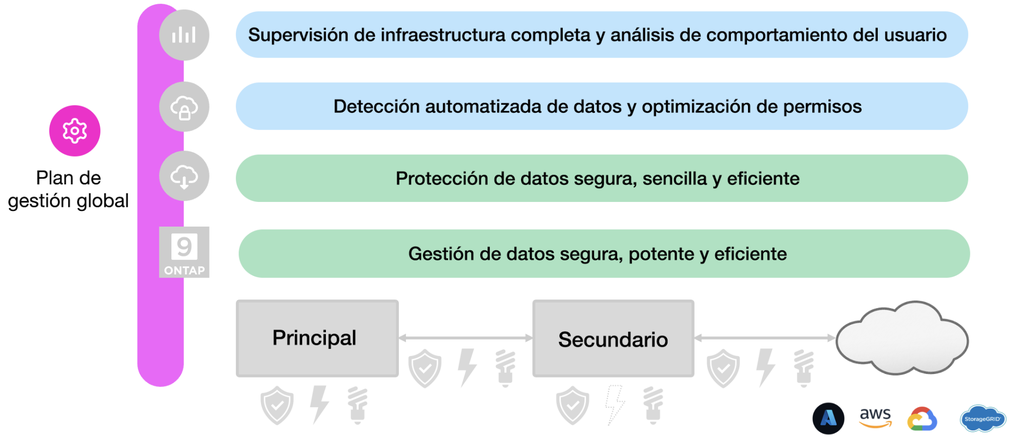
Detectar y combatir toda esta actividad sería difícil para unos pocos individuos, especialmente si tienen que compaginar otras responsabilidades en una zona horaria diferente. Pero el equipo de TI cuenta con NetApp Cloud Insights para supervisar los archivos compartidos en red y detectar las anomalías de los usuarios. Incluso si el equipo no se da cuenta del ataque, Cloud Insights sí lo ve y crea al instante una copia de Snapshot™ de NetApp para proteger los datos.

Es posible que tu volumen principal se vea afectado por el cifrado, pero tus copias de Snapshot son inmutables y cuando se combinan con Cloud Backup de NetApp ofrecen una estrategia de protección de datos segura y eficaz.

Cloud Insights puede identificar la fuente la fuente del ataque y bloquear la cuenta del usuario comprometido para evitar daño adicional y ayudar a evitar la filtración de datos.

¿Qué pasa con ese malware que va poco a poco desplazándose por tu almacenamiento de archivos? No hay problema. Se envía una alerta gracias a la protección contra ransomware autónoma integrada en ONTAP, que usa aprendizaje automático para supervisar la actividad de carga de trabajo y la entropía de datos. Esta alerta también activa una copia Snapshot automática, lo que proporciona varios puntos de recuperación.

Los ataques de suplantación de identidad y los adjuntos por correo electrónico no son las únicas amenazas. Las credenciales de administración comprometidas o, aún peor, los administradores malintencionados, pueden poner tus datos en un riesgo serio. ONTAP de NetApp puede evitar que una única cuenta de administrador cause daños al requerir que más de una cuenta de administrador apruebe tareas cruciales, como eliminar copias de Snapshot usando la nueva función de verificación multiadministrador.



## Restauración

Con Cloud Data Sense y Cloud Insights, puedes aplicar técnicas forenses de archivos inteligentes para identificar los datos que se vieron afectados y quién está detrás de ello. De esa forma, podrás centrarte en la recuperación de datos y reducir el tiempo de inactividad.

A continuación, el equipo de TI puede proceder a restaurar datos rápidamente en cuestión de minutos utilizando las herramientas de NetApp. Se pueden exportar los registros a software de gestión de eventos e información de seguridad líder para poder realizar más análisis.

A pesar del dramático panorama del momento, todo el equipo tiene la seguridad de que se recuperarán los datos, porque el software SnapLock® de NetApp usa bloqueo de archivos WORM seguro para evitar la eliminación de los datos.

# Un plan de resiliencia cibernética centrado en los datos, dondequiera que residan

¿Sigue siendo válido el escenario anterior si tu equipo de TI gestiona los datos de manera local? ¿En el cloud? ¿En un entorno híbrido? ¿En el perímetro? Desde luego.

Como la resiliencia cibernética está diseñada para centrarse en los datos, tus datos están siempre seguros, resilientes y disponibles, independientemente de si están en las instalaciones, en una ubicación remota o en el cloud. La solución de resiliencia cibernética de NetApp abarca el cloud híbrido y se integra con los principales clouds públicos.

## Aprovecha al máximo tu inversión actual

La solución de resiliencia cibernética de NetApp centrada en los datos puede ayudar en las cinco etapas del plan que hemos descrito aquí. Pero es posible que tu empresa ya haya invertido en otras herramientas de ciberseguridad. Las funciones del software ONTAP de NetApp pueden integrarse con las inversiones existentes en ciberseguridad, de modo que puedes cerrar las brechas en lugar de empezar completamente de cero.

### Protección de datos

Integración con ONTAP® Snapshot™ de NetApp® y replicación eficiente con SnapMirror®

COMMVAULT, rubrik, veeam, CLEONDRIS, CATALOGIC SOFTWARE, IBM, ProLion, VERITAS

### Comportamiento del usuario

Integración con las API de FPolicy para ofrecer una visión inteligente del comportamiento de los archivos y los usuarios

Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits TECHNOLOGIES, VARONIS, VERITAS, splunk>

### Auditoría y registro

Integración con herramientas syslog o SIEM de análisis forense

Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits TECHNOLOGIES, VARONIS, VERITAS, splunk>

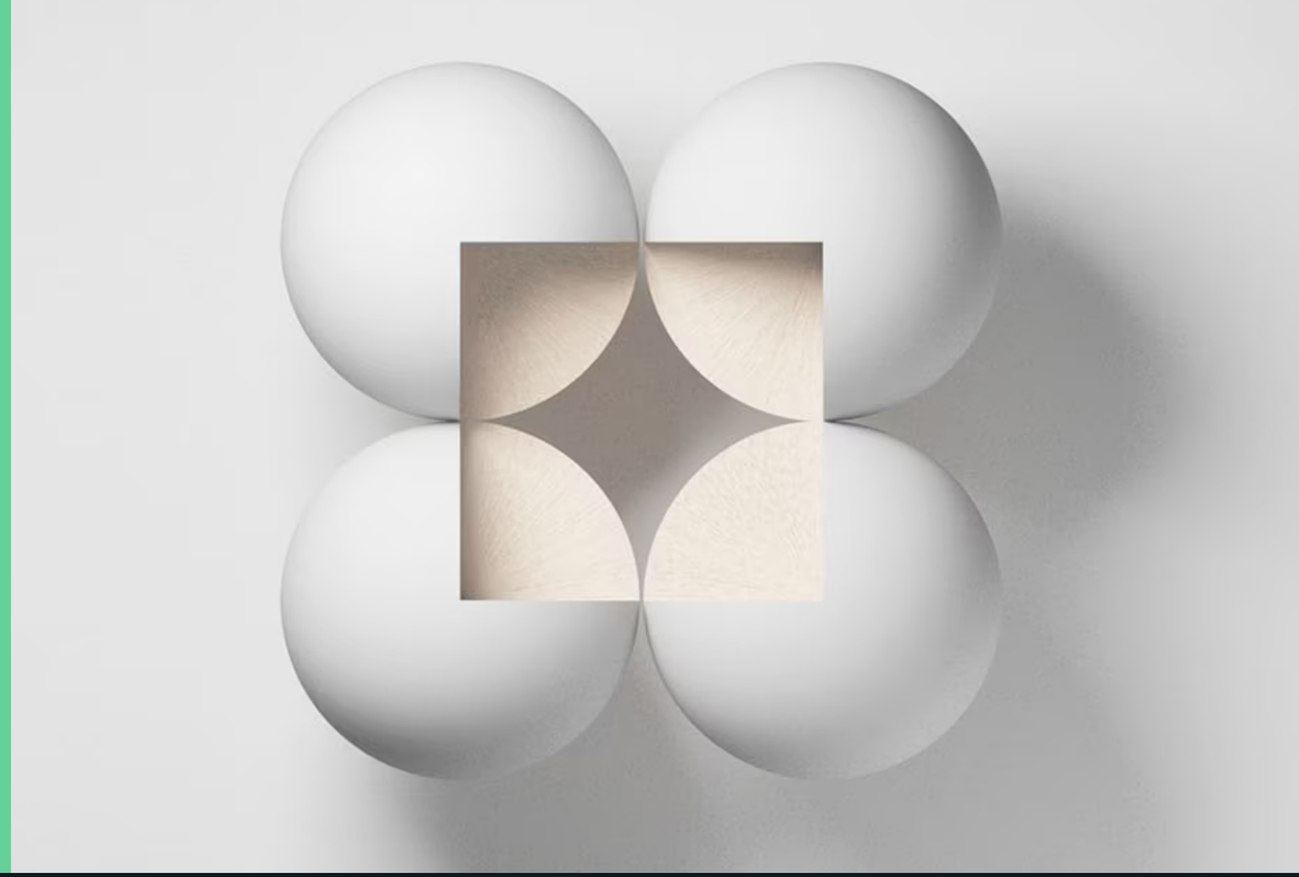
# Estás a unos pocos clics de tu plan de resiliencia cibernética

No podemos eliminar a los delincuentes, pero podemos activar la resiliencia cibernética de tu organización con las herramientas adecuadas.

Obtén más información acerca de cómo NetApp te puede ayudar a poner en acción tu plan de resiliencia cibernética centrada en los datos.
**netapp.com/cyber-resilience/**

# Haz clic en los siguientes enlaces para ver las soluciones de resiliencia cibernética, los blogs y los vídeos más recientes de NetApp

- Soluciones de resiliencia cibernética de NetApp
- Soluciones de protección de datos de NetApp
- Soluciones de ransomware de NetApp
- Blogs de resiliencia cibernética de NetApp
- Vídeos de resiliencia cibernética de NetApp.tv




1. National Institute for Standards and Technology, “Desarrollo de sistemas con resiliencia cibernética,” (en inglés) diciembnre de 2021.
2. PBS NewsHour, , «Why ransomware attacks are on the rise—and what can be done to stop them», 8 de julio de 2021.
3. Business Wire, «Ransomware Index Spotlight Report Reveals Steady Increase in Sophistication and Volume of New Ransomware Vulnerabilities and Families in Q3 2021», 9 de noviembre de 2021.
4. Statista, Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021». 2021.
5. Sophos News, «The State of Ransomware 2021», 27 de abril de 2021.
6. Deloitte, «Double extortion incidents», octubre de 2020.
7. Infosec, «NIST CSF: Implementing NIST CSF», 19 de febrero de 2020.


**Acerca de NetApp**
En un sector lleno de generalistas, NetApp es un especialista. Nos centramos en una cosa: ayudar a tu empresa a aprovechar al máximo sus datos. NetApp incorpora al cloud los servicios de datos de clase empresarial en los que confías, y lleva la sencilla flexibilidad del cloud al centro de datos. NetApp incorpora al cloud los servicios de datos de clase empresarial en los que confías, y lleva la sencilla flexibilidad del cloud al centro de datos.

Como empresa de software centrado en datos y orientado al cloud, solo NetApp puede ayudarte a crear un Data Fabric exclusivo, a simplificar y conectar tu cloud y a proporcionar con seguridad los datos, los servicios y las aplicaciones correctos a las personas adecuadas en cualquier momento y lugar.

NetApp

+1 877 263 8277



NA-817-0622-esES