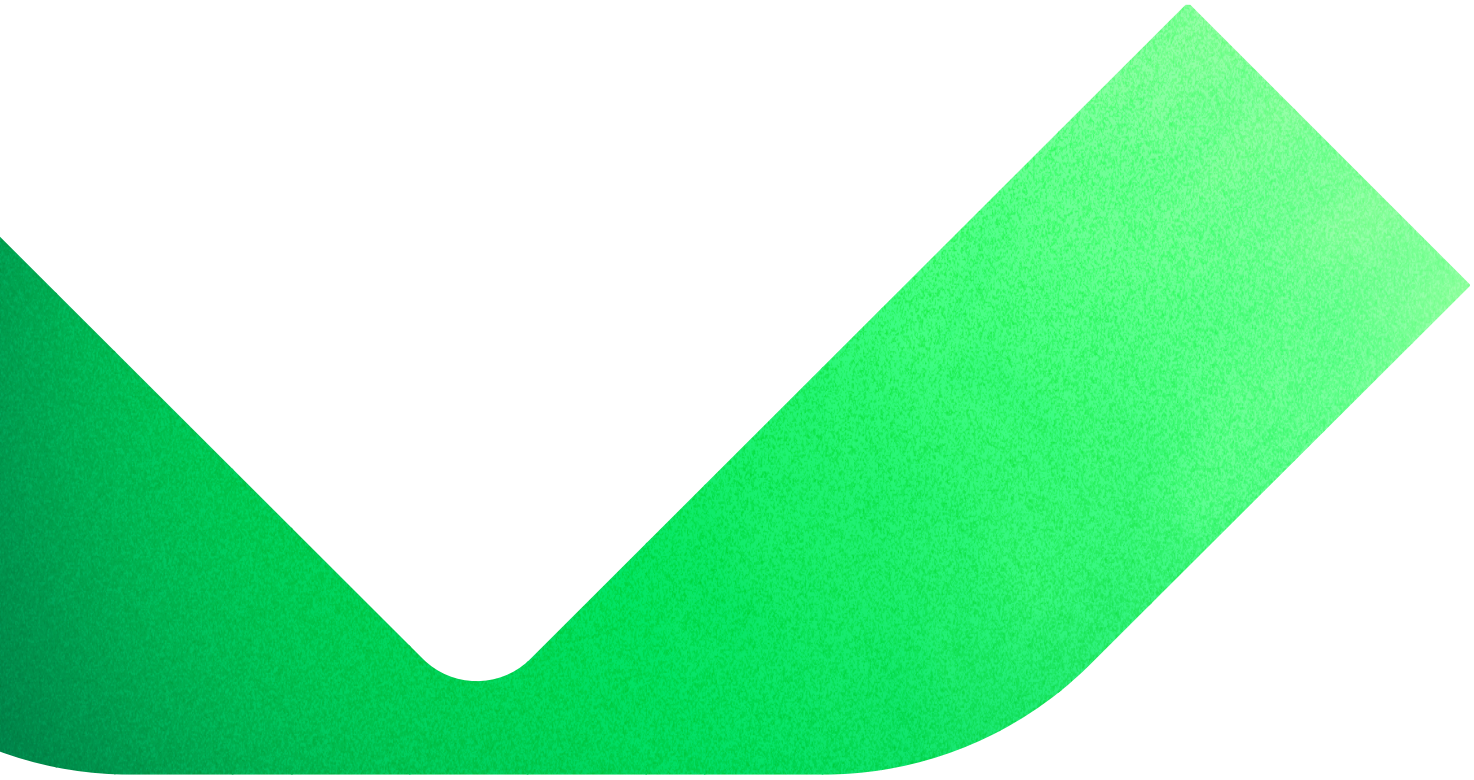
Resiliencia de datos Zero Trust

Un modelo de backup y recuperación de datos seguro



Contenido

Resumen ejecutivo

En la actualidad, las empresas se enfrentan a importantes desafíos para proteger sus datos y redes de los actores maliciosos, en particular contra el ransomware y los ataques de exfiltración de datos. Para abordar estas preocupaciones, una estrategia conocida como Zero Trust ha cobrado un impulso significativo en la industria de la seguridad de la información y está siendo ampliamente adoptada por las empresas de todo el mundo.

Sin embargo, incluso los modelos Zero Trust más utilizados carecen de directrices completas en ciertas áreas importantes, especialmente en lo que respecta al backup y la recuperación de los datos. Conscientes de la importancia de solucionar esta carencia y aplicar los principios de Zero Trust en esta área, presentamos el concepto de Resiliencia de datos de Zero Trust. Esto se compone de un conjunto de requisitos, una arquitectura y una extensión de los modelos de madurez de confianza cero existentes.

En concreto, las empresas deben usar un sistema de backup y recuperación de los datos que proporcione almacenamiento de datos y configuración inmutables y exija al mismo tiempo un acceso contextual y con funciones de autenticación muy seguras a los datos de origen en producción y a los datos del backup. Este sistema también debe soportar sin problemas las arquitecturas híbridas comunes en las empresas actuales y manejar la recuperación de manera flexible en entornos disímiles.

Al implementar una arquitectura Zero Trust que cumpla con estos requisitos, las empresas protegerán mejor sus datos, redes y aplicaciones frente a actores maliciosos. Zero Trust proporciona una seguridad manifiestamente mejor en comparación con los enfoques tradicionales, y las organizaciones se ven en la obligación de adoptarla. Los nuevos requisitos de resiliencia de datos propuestos en este white paper mejoran y amplían el principio de Zero Trust (confianza cero), y deben considerarse obligatorios dentro de la estrategia de seguridad de cualquier empresa.

Introducción

Zero Trust es una estrategia de seguridad y, por necesidad, tiene un amplio alcance. Sin embargo, los modelos y marcos de Zero Trust que se utilizan de forma generalizada no incluyen todo[1]. Esto puede dar lugar a las correspondientes brechas u omisiones en las arquitecturas de seguridad de las empresas. Específicamente, los sistemas de backup y recuperación de los datos no se incluyen en los marcos de trabajo Zero Trust más utilizados. Y esto constituye una brecha desafortunada, ya que los datos empresariales son con mucha frecuencia el objetivo principal de los actores maliciosos tanto en los ataques de ransomware como en los de exfiltración de datos.

Los sistemas de backup y recuperación de datos son elementos fundamentales de la TI empresarial y deben tratarse como tales. Tienen acceso de lectura a todo lo que es importante para realizar un backup. También necesitan la capacidad de escribir datos en entornos de producción para llevar a cabo su función de restauración de datos. Además, contienen una copia completa de los datos más importantes de la empresa. Tomados en conjunto, todos estos atributos subrayan la importancia de los sistemas de backup y recuperación de datos, y resaltan su valor como objetivo para los actores maliciosos.

Por supuesto, los sistemas de backup y recuperación de los datos han formado parte de la tareas del departamento de TI durante décadas, pero a menudo no se han incluido en el ámbito o la responsabilidad de los equipos de seguridad. Sin embargo, dado el nivel y la sofisticación de las amenazas de seguridad a las que se enfrentan actualmente las empresas, ya no basta con adoptar únicamente una perspectiva de infraestructura de TI y red para el backup y la recuperación de datos. En la práctica, nos hemos encontrado con empresas en las que estos sistemas estaban mal configurados y no estaban supervisados, por lo que suponían un riesgo significativo.

La seguridad moderna y eficaz se basa en los principios Zero Trust, por lo que es hora de revisar los sistemas de backup y recuperación de datos desde ese punto de vista. Este white paper lo consigue al proponer un nuevo concepto de Resiliencia de datos Zero Trust. Al adoptar este enfoque, las empresas podrán seguir un rumbo claro y preciso para disponer de sistemas defensivos más fuertes, operaciones más eficientes y una recuperación más rápida.

[1] El documento CISA ZTMM establece que "si bien la ZTMM abarca muchos aspectos de la ciberseguridad críticos para las empresas federales, no aborda otros aspectos de la ciberseguridad como... la recuperación".

Enfoque

Los elementos fundamentales clásicos de la seguridad de la información, la tríada CIA de Confidencialidad, Integridad y Disponibilidad, son aplicables al backup y recuperación de datos. Las empresas deben evitar la filtración de datos (Confidencialidad), impedir que el ransomware cifre los datos (Integridad) y garantizar que los sistemas estén protegidos contra ataques y que puedan restaurarse rápidamente después de un ataque (Disponibilidad).

Los principios básicos de Zero Trust son ciertamente relevantes para este dominio, y deben aplicarse al acceso de los usuarios y a los sistemas de TI de las empresas, así como a los sistemas de backup y recuperación de los datos. Estos principios incluyen la eliminación de la confianza implícita y las redes sin segmentar, el control de todos los accesos mediante políticas dinámicas y contextuales a través de puntos de aplicación de políticas (PEP), la exigencia de una autenticación debidamente segura de todos los sujetos, la aceptación de la vulnerabilidad y la garantía y validación de la integridad del sistema y de los datos. A lo largo de este white paper, veremos cómo estos principios se trasladan al nuevo conjunto de requisitos propuesto para una arquitectura de Resiliencia de datos Zero Trust.

El marco estándar de facto para analizar la madurez de Zero Trust es el Modelo de Madurez Zero Trust de CISA[2] que se muestra en la Figura 1, el cual define cinco pilares básicos: Identidad, Dispositivos, Redes, Aplicaciones y Cargas de Trabajo, y Datos. También define tres funcionalidades transversales: Visibilidad y análisis, Automatización y orquestación, y Gobernanza.

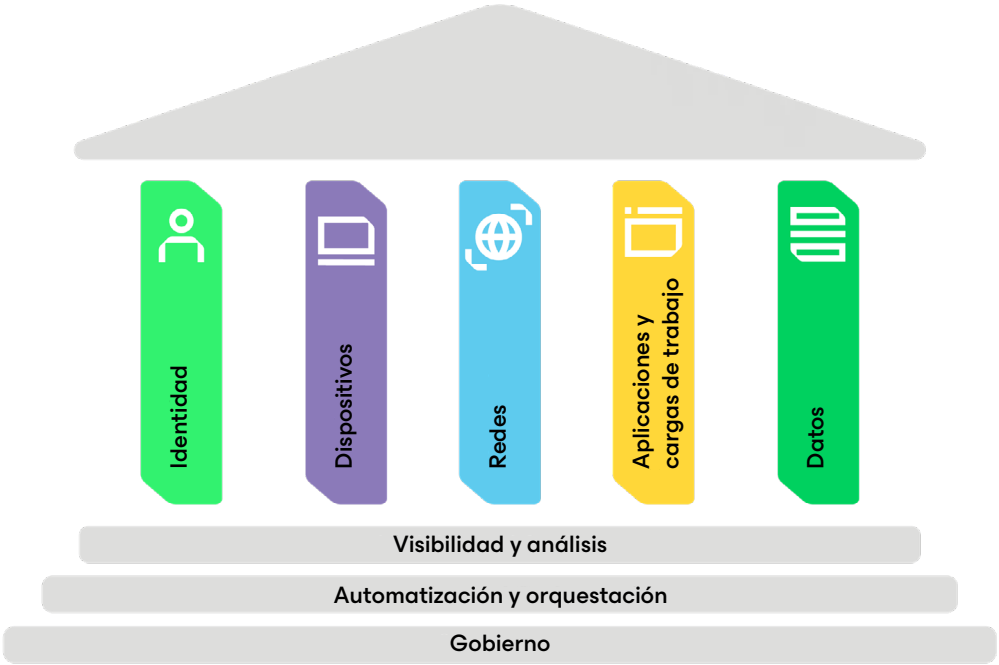


Figura 1: Modelo de Madurez Zero Trust de CISA

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Dentro del pilar de datos, el modelo CISA identifica cinco funciones detalladas, con funcionalidades y atributos esperados para cada nivel de madurez.

Sin embargo, dentro de estas funciones, el tema de la integridad del backup y la recuperación es mínimo, y CISA remite a los lectores a un documento del NIST de 2020 que no está relacionado con Zero Trust. En resumen, el modelo CISA Zero Trust no dice nada sobre los requisitos y niveles de madurez para los sistemas de backup y recuperación de datos. Dado que esta área es tan importante para la confidencialidad, integridad y disponibilidad de la empresa, creemos que es necesario abordar esta brecha.

Para ello, presentamos el concepto de Resiliencia de datos Zero Trust, que incluye algunos principios, una arquitectura de referencia y un nuevo conjunto de funcionalidades para el Modelo de Madurez de Zero Trust. En conjunto, representan una ampliación y mejora de Zero Trust y darán como resultado una postura de seguridad de la empresa más sólida.

Las funciones son:

- Gestión de inventario de datos
- Categorización de datos
- Disponibilidad de los datos
- Acceso a los datos
- Cifrado de datos

Resiliencia de datos de confianza cero (Zero Trust): principios

Los principios de la Resiliencia de datos Zero Trust (ZTDR) son:

Acceso de privilegio mínimo

Inmutabilidad

Resiliencia del sistema

Validación proactiva

Simplicidad operativa

Analicemos cada uno de estos a su vez.

Acceso de privilegio mínimo

Este principio es fundamental para Zero Trust y es una parte necesaria de cualquier arquitectura Zero Trust. Sin embargo, vale la pena examinar su aplicabilidad a las características específicas de ZTDR, ya que se utiliza en varios niveles. Desde una perspectiva de red, el propio sistema de administración de backup debe estar aislado en la red para que ningún usuario o dispositivo no autenticado o no autorizado pueda acceder a él. De igual forma, el sistema de almacenamiento de backup debe estar aislado. Esto evita que los actores maliciosos descubran cualquiera de los sistemas a través del reconocimiento de la red o explotando una vulnerabilidad.

El acceso legítimo y autorizado al sistema de backup solo debe producirse a través de un Punto de Aplicación de la Política de Confianza Cero (PEP) con una autenticación adecuadamente sólida y comprobaciones de la postura del dispositivo. El PEP Zero Trust también debe controlar el acceso a los datos de origen (es decir, los datos de los que se hace backup), con la autenticación adecuada y cierto nivel de validación del dispositivo o sistema para garantizar que el sistema de gestión de copias de seguridad sea el que lea los datos de producción, en lugar de un sistema o proceso malicioso.

El acceso desde el sistema de gestión de backup al almacenamiento de backup también debe controlarse mediante un PEP y segmentarse del resto de la red con una autenticación suficientemente fuerte. Tenga en cuenta que revisaremos este requisito en el diagrama de arquitectura a continuación, ya que es importante: el sistema de almacenamiento de backup debe estar segmentado del sistema de administración de backup.

Inmutabilidad

El concepto y requisito para los datos de backup inmutables se ha adoptado de forma generalizada en los últimos años, junto con el crecimiento de la prevalencia y sofisticación del ransomware. Un backup inmutable se define como aquellos datos de los que se ha hecho backup utilizando un mecanismo de almacenamiento que, una vez escrito, no puede modificarse. La premisa es que, incluso si un actor malicioso estuviera presente en la red y pudiera tomar el control del sistema de backup y tener acceso al almacenamiento de backup, no podría eliminar o modificar (cifrar) los datos respaldados. Parte de la inmutabilidad proviene de las propiedades físicas de los medios de almacenamiento, como los discos ópticos Write-Once-Read-Many, en tanto que las tecnologías más recientes utilizan medios con inmutabilidad aplicada en las capas de hardware, firmware o software. Más recientemente, los principales proveedores de servicios cloud han agregado funcionalidades de almacenamiento inmutable para satisfacer los requisitos de cumplimiento y archivado de las empresas.

NOTA

Los requisitos para la inmutabilidad se extienden más allá de los datos almacenados, y deben incluir también los periodos de retención de datos. Algunos datos inmutables pueden configurarse para un almacenamiento indefinido, mientras que otros pueden tener un período de retención definido, como uno o cinco años. Los datos que envejecen más allá de su periodo de retención pueden eliminarse, por lo que el sistema de almacenamiento de datos también debe hacer que el periodo de retención de los datos sea inmutable. Esto elimina el acortamiento malintencionado de los períodos de retención.

Resiliencia del sistema

Tenemos una visión bastante amplia de la resiliencia de los sistemas y creemos que debe aplicarse no solo a la infraestructura de backup en sí, sino a todo el ecosistema de herramientas, tecnologías y procesos relacionados con el backup y la recuperación de datos. Concretamente, la infraestructura de backup debe ser resiliente a fallos y ataques, como la falta de disponibilidad de los componentes o de la red, o la manipulación del servidor de tiempo de red (NTP) para que caduquen de forma malintencionada los datos de backup. También debe ser fácil configurar el uso del almacenamiento de datos de backup distribuido y heterogéneo; por ejemplo, entre geografías o tipos de infraestructura. La resiliencia también se mejora al separar los datos de backup del sistema de administración de backup, de modo que si se compromete el sistema de backup no se comprometerá también el almacenamiento de datos. De hecho, debe buscar un sistema de gestión de backups que, en caso de compromiso o fallo, pueda volver a constituirse sin afectar a su capacidad para acceder a los datos del backup y restaurarlos.

El sistema también debe ser resistente a los cambios esperados e inesperados en el entorno empresarial. Los cambios esperados incluyen la incorporación o eliminación planificada de componentes de infraestructura, como la adopción de aplicaciones y datos híbridos o basados en la nube. Es decir, el sistema de backup debe ser capaz de capturar y almacenar eficientemente los datos empresariales, independientemente de su ubicación de origen o tecnología. Los cambios inesperados normalmente se producen durante la respuesta a incidentes o la recuperación ante desastres (DR), y por lo general se categorizan como soporte para la recuperación en entornos diferentes. Cuando una organización está recuperando datos, es muy posible que el entorno de recuperación se ejecute en una ubicación o tipo de infraestructura diferente. Por ejemplo, un centro de datos en las instalaciones locales inundado puede requerir la recuperación a un entorno basado en la nube, y situar allí las operaciones en curso durante un período de tiempo prolongado. Por lo tanto, el sistema de backup debe admitir tanto la recuperación en este entorno diferente como los nuevos backups desde este entorno de producción en adelante.

El propio sistema de almacenamiento de datos de backup, además de proporcionar almacenamiento de datos inmutable, debería endurecerse fácilmente. Esto puede adoptar la forma de un dispositivo pre-reforzado o un sistema configurable por el administrador con recomendaciones claras de endurecimiento, que será más adecuado para empresas avanzadas.

Validación proactiva

Garantizar el correcto funcionamiento del sistema requiere que se supervise el sistema y se validen todos los aspectos funcionales y los procesos. Esto tiene dos aspectos. En primer lugar, el sistema de backup debe ser supervisado en términos de red, rendimiento y seguridad. Es decir, este sistema debe ser tratado como cualquier otro sistema de producción de alto valor.

En segundo lugar, y lo más importante, se debe confirmar periódicamente la validez de los datos de los que se ha hecho backup, así como la fiabilidad y la eficacia de los procesos de recuperación. Por definición, la recuperación de los datos respaldados va a ocurrir en momentos inesperados y probablemente en un entorno de alto estrés. Es importante que la organización tenga un proceso bien entendido, bien documentado y bien ensayado. También es necesario que haya varias personas capaces de realizar esto para tener en cuenta las vacaciones, la falta de disponibilidad y la rotación del personal.

Tenga en cuenta que, si bien esto requiere una inversión de tiempo y energía, esto demuestra madurez operativa, y es una "póliza de seguro" en caso de desastre. Tenga en cuenta también que "desastre" no tiene por qué significar un desastre literal o un evento importante como la inundación de un centro de datos. Por ejemplo, una empresa con la que trabajamos experimentó un flujo de trabajo automatizado descontrolado debido a un error de programación, lo que resultó en la eliminación de cantidades significativas de datos de producción en su sistema de administración financiera. Esto no fue un desastre literal, y se evitó que se convirtiera en un desastre en sentido figurado usando sus procesos de recuperación de datos (validados).

Además, el sistema de gestión de backups debe tener la capacidad directa o indirecta de organizar los backups a lo largo de una línea de tiempo de infección de malware. Es decir, debería ser capaz de detectar (o ser informado de) infecciones de malware y clasificar los backups como limpios, dudosos o comprometidos, dependiendo de cuándo fueron capturados.

NOTA

Los procesos de validación y recuperación de datos también deben respetar los requisitos de privacidad y residencia de datos. Esto puede agregar complejidad y riesgo, por lo que debe hacerse con cuidado, con conocimiento del contenido de los datos y de las obligaciones legales y de cumplimiento de la organización.

Simplicidad operativa

Nuestro principio final es la simplicidad operativa, que definimos como un sistema que es lo suficientemente fácil para que su organización opere con confianza y, al mismo tiempo, proporciona suficiente capacidad, escalabilidad y sofisticación para satisfacer plenamente las necesidades de su empresa. Es decir, un sistema adecuado para su organización.

Esto es importante: hemos visto que las empresas luchan por usar y poner en funcionamiento sistemas que son demasiado complejos para el tamaño, el equipo, las habilidades y las necesidades de su organización. Esto genera beneficios limitados, frustración e incapacidad para ofrecer madurez de seguridad o valor comercial. Un conjunto de atributos que hay que buscar en un proveedor de backup es su fortaleza relativa a la orquestación y automatización. Los proveedores con funcionalidades sólidas en sus plataformas serán más rápidos y fáciles de operar.

Para concluir esta sección, cada uno de estos principios está insertado en las ampliaciones del nuevo Modelo de Madurez que se analizan más adelante en este documento, y también serán evidentes en la arquitectura de referencia que analizamos a continuación.

Resiliencia de datos de confianza cero (Zero Trust): arquitectura de referencia

Las arquitecturas de backup de datos variarán, necesariamente, entre las diferentes empresas, dada la enorme variabilidad de las infraestructuras de red, aplicaciones y datos, entre otros factores. Aun así, existen elementos arquitectónicos comunes debido a los principios comunes de Zero Trust que deben estar presentes en cualquier arquitectura de Resiliencia de datos Zero Trust.

Nuestra arquitectura de referencia se muestra en la Figura 2 e ilustra los requisitos clave en este tipo de sistema. Tenga en cuenta que esto representa el entorno desde la perspectiva del sistema de administración de backup. El acceso regular y cotidiano de los usuarios y los sistemas a los sistemas de producción también estaría controlado por PEP de Zero Trust, pero esto se omite en el diagrama para mayor claridad.

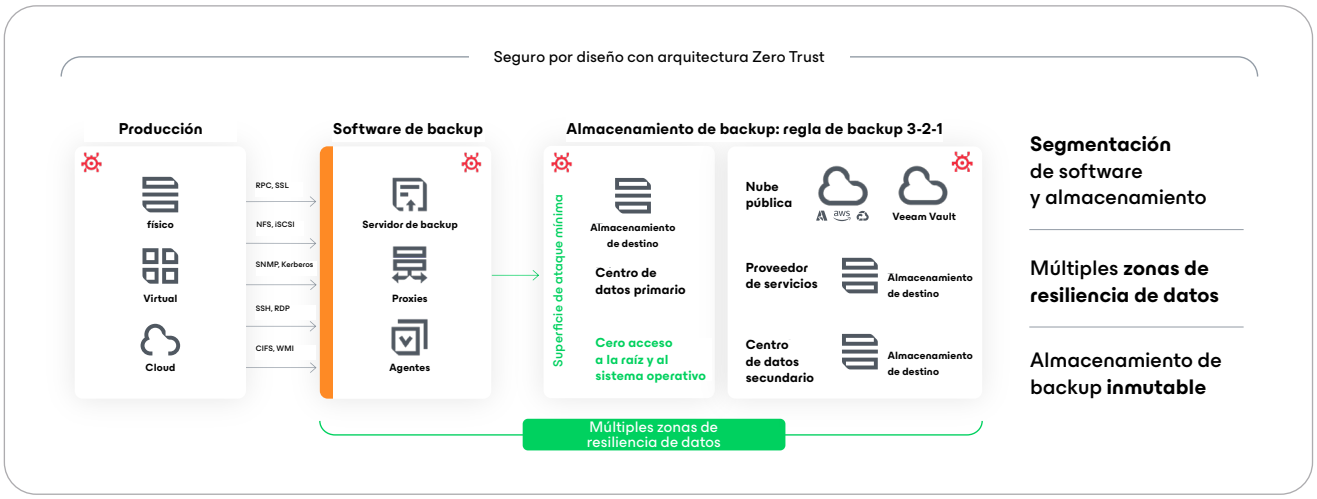


Figura 2: Resiliencia de datos de confianza cero (Zero Trust): arquitectura de referencia

En primer lugar, observe las partes centrales de cualquier arquitectura Zero Trust: el Punto de decisión de políticas (PDP) centralizado, que delega la autenticación de identidad en el sistema Identity and Access Management (IAM) de la empresa. El PDP se basa en su almacén de directivas para tomar decisiones de acceso a las identidades autenticadas, incluidas las identidades humanas y no humanas (sistema). En esta arquitectura, el PDP toma decisiones de acceso para el sistema de administración de backup. Estas decisiones se comunican a través del plano de control (mostrado como líneas punteadas) con los puntos de aplicación de políticas (PEP), que se sitúan lógicamente en línea entre el sistema de gestión de backup y las fuentes de datos de las que se va a hacer backup y las ubicaciones de backup de destino.

La arquitectura también incluye una estructura recomendada para los datos respaldados. Además del requisito de inmutabilidad de datos, las empresas deben intentar mantener al menos una copia en una ubicación principal que tenga una conexión de red de baja latencia con el sitio de restauración previsto. Esto permite obtener snapshots de backup rápidos, que fomentan puntos de recuperación más frecuentes y tiempos de recuperación más rápidos. Obviamente, la ubicación principal suele estar situada junto con los sistemas de producción, por lo que nuestra arquitectura de referencia también ilustra el objetivo de tener al menos 2 copias de los datos en ubicaciones secundarias[3]. Estos deben estar geográficamente aislados de la ubicación principal para lograr la resiliencia frente a un desastre regional. La contrapartida más probable es una conexión de red más lenta, que puede dar lugar a puntos de recuperación de menor frecuencia y tiempos de recuperación más largos.

NOTA

El sistema de administración de backup está deliberadamente separado de sus niveles de almacenamiento. Esto permite al sistema de backup distribuir sin problemas los datos de los que se ha hecho backup entre múltiples repositorios inmutables y distribuidos geográficamente. También permite a las empresas seleccionar los repositorios de almacenamiento de backup que ofrezcan la mejor combinación de rendimiento, precio y simplicidad operativa para sus necesidades únicas. También proporciona una capa adicional de seguridad al controlar la comunicación a través de un PEP.

[3] Existen varias escuelas de pensamiento en torno al número de backups en varias ubicaciones, a menudo referidas a través de recursos mnemotécnicos como 3-2-1 o 3-2-1-1-0.

Resiliencia de datos de confianza cero (Zero Trust): Modelo de Madurez Ampliado

Aunque los principios y la arquitectura de referencia que hemos propuesto para la resiliencia de datos de confianza cero son de aplicación universal, no pueden aplicarse completa e inmediatamente a la mayoría de las empresas. Como la mayoría de los aspectos de Zero Trust, deben planificarse y adoptarse de forma incremental. La forma estándar de modelar y comunicar esto es a través de un modelo de madurez. Como mencionamos en la introducción, estamos siguiendo el framework estándar de facto del Modelo de Madurez de Zero Trust de CISA y lo estamos ampliando con cuatro nuevas funciones que abarcan nuestros principios y requisitos.

Estas nuevas funciones son:

Acceso a los datos y sistemas de la empresa

Acceso a almacenamiento y datos de backup

Resiliencia del sistema

Monitorización y validación del sistema

Estas extensiones ZTDR del modelo de madurez se representan en las Figuras 3 a 6, que muestran cómo se debe avanzar en cada una de las cuatro nuevas funciones a través de los niveles de madurez estándar: Tradicional, Inicial, Avanzado y Óptimo.

Para cada una de las funciones, hemos identificado los atributos esperados para cada nivel de madurez. De este modo, el modelo representa las mejoras y cambios que una organización necesita realizar para avanzar en la madurez de cada función. A continuación, examinaremos por turnos cada una de las funciones a medida que va pasando por los diferentes niveles de madurez.

Acceso a los datos y sistemas de la empresa

Esta función se define como los medios y mecanismos mediante los cuales el sistema de administración de backup (BMS) tiene acceso a los datos de origen cuyo backup se encarga de realizar.

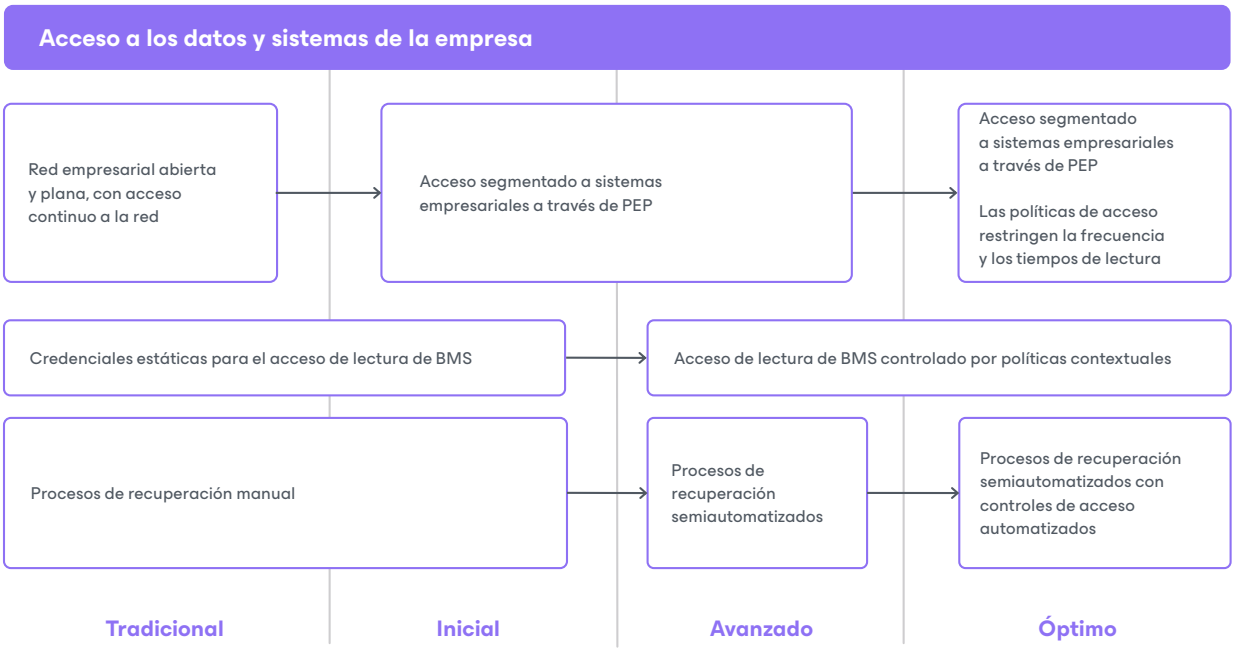


Figura 3 - Acceso a los datos y sistemas de la empresa: Modelo de Madurez

En el nivel de madurez **Tradicional**, la empresa tiene una red plana y abierta, y el sistema de administración de backup tiene acceso de red continuo y sin obstáculos a los sistemas fuente. El BMS utiliza credenciales estáticas, como una clave de API, un nombre de usuario/contraseña almacenados o un certificado, para autenticar y leer los datos de origen. Cuando la empresa utiliza el BMS para recuperar un sistema, se basa en procesos manuales.

Para avanzar al nivel **Inicial**, la empresa debe comenzar a aplicar una mejor segmentación de la red y restringir el acceso de BMS a los sistemas empresariales a través de un Punto de aplicación de políticas de Zero Trust, introduciendo el principio de privilegio mínimo.

Cuando la empresa se encuentre en el nivel **Avanzado**, habrá introducido políticas de acceso contextual para el acceso de BMS a los datos y sistemas de la empresa, utilizando mejor así las funcionalidades dinámicas de aplicación de políticas de Zero Trust. También habrán comenzado a utilizar procesos de recuperación automatizados con algunos pasos manuales para el inicio y la validación del proceso.

En el nivel **Óptimo**, la organización habrá mejorado el uso de las políticas de acceso para restringir el acceso de BMS solo a los períodos de tiempo permitidos o a los eventos de recuperación activos. Esto refuerza aún más el principio de privilegio mínimo.

Acceso a almacenamiento y datos de backup

Esta función se define como los medios y mecanismos por los cuales el sistema de administración de backup tiene acceso de escritura y lectura al almacenamiento de backup y a los datos almacenados allí.

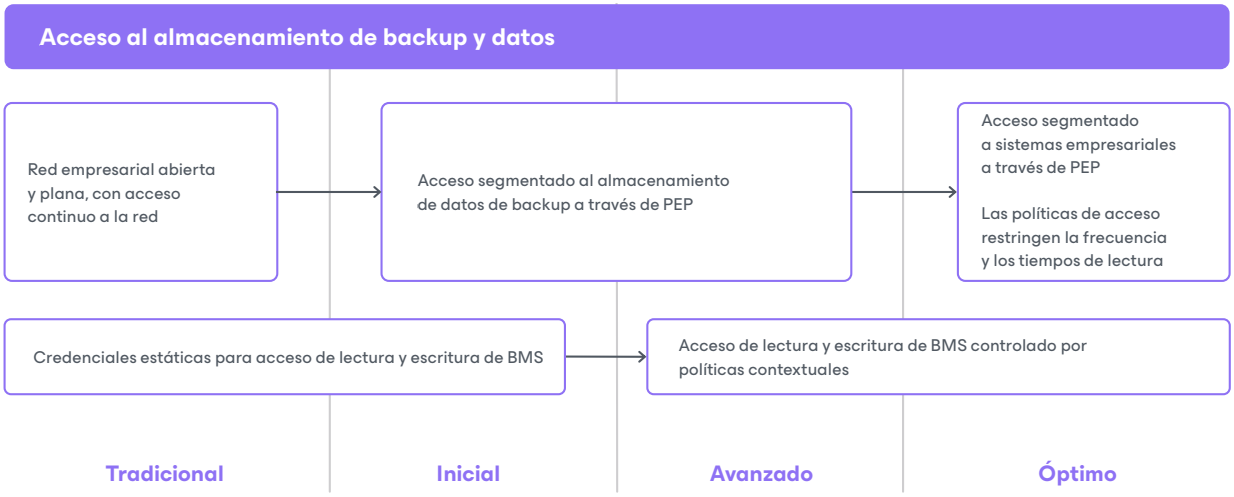


Figura 4 - Acceso al almacenamiento de backup y datos: Modelo de Madurez

En el nivel de madurez **Tradicional**, la empresa cuenta con una red plana y abierta, y el sistema de administración de backup tiene acceso de red continuo y sin obstáculos al sistema de almacenamiento de backup y a los datos de backup almacenados allí. El BMS utiliza credenciales estáticas, como una clave de API, un nombre de usuario/contraseña almacenados o un certificado, para autenticarse y escribir en el almacenamiento, y leer los datos almacenados.

Para avanzar al nivel **Inicial**, la empresa debe comenzar a aplicar una mejor segmentación de la red y restringir el acceso de BMS al almacenamiento de backup y a los datos almacenados a través de un Punto de Aplicación de la Política de Confianza Cero (Zero Trust), haciendo cumplir el principio de privilegio mínimo.

Cuando la empresa se encuentre en el nivel **Avanzado**, habrá introducido políticas de acceso contextual para el acceso de BMS al sistema de almacenamiento de backup y a los datos almacenados. De esta forma, se aprovechan mejor las funcionalidades dinámicas de aplicación de políticas dentro de la empresa.

En el nivel **Óptimo**, la organización habrá mejorado el uso de las políticas de acceso para restringir el acceso de BMS al almacenamiento solo a los períodos de tiempo permitidos o durante los eventos de recuperación activos. Esto refuerza aún más el principio de privilegio mínimo.

Resiliencia del sistema

Esta función se define como las características del sistema de backup con respecto a su resistencia a fallas del sistema, fallas de componentes o actividades maliciosas.

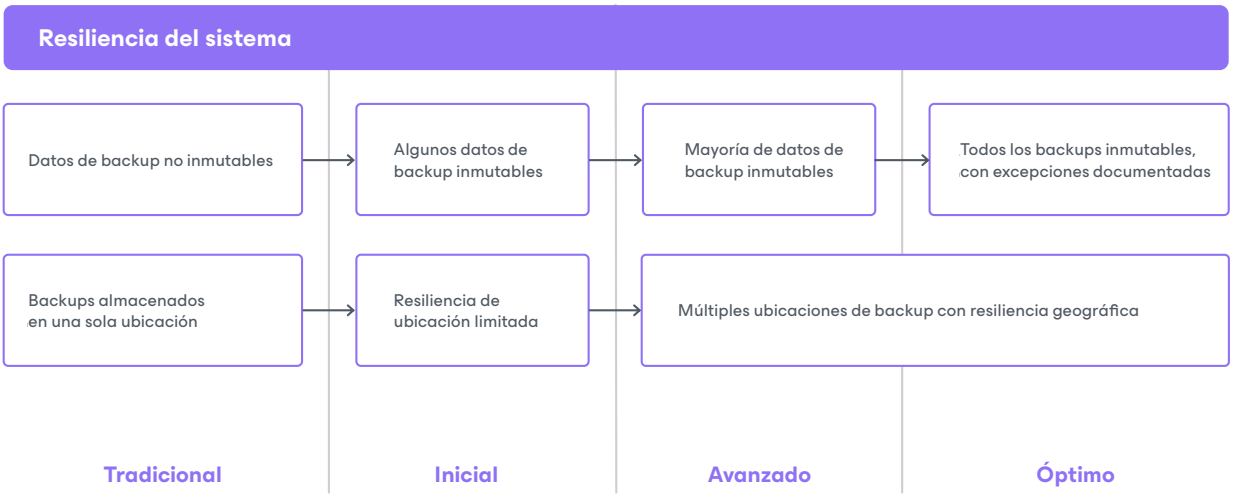


Figura 5 - Resiliencia del sistema: Modelo de Madurez

En el nivel de madurez **Tradicional**, la organización usa almacenamiento mutable para los datos de backup, lo cual pone en riesgo su integridad y disponibilidad. Por lo general, también almacenan backups en una sola ubicación, lo que somete a la organización a una pérdida total en caso de un desastre regional.

A medida que la organización avanza al nivel **Inicial**, debe empezar a usar almacenamiento inmutable para algunos de sus backups de datos e introducir cierta resiliencia de ubicación limitada para esos backups.

En el nivel **Avanzado**, la organización usará fundamentalmente almacenamiento de backup inmutable, con prioridades idealmente establecidas en función de la sensibilidad de los datos y la importancia crítica. También habrán introducido y puesto a funcionar varias ubicaciones de almacenamiento de backup, en geografías distribuidas.

Cuando la empresa se encuentre en el nivel **Óptimo**, habrá pasado a usar almacenamiento de backup inmutable por completo, con algunas excepciones documentadas y aprobadas. Las nuevas fuentes de datos y aplicaciones usarán de forma predeterminada el backup inmutable. Este nivel proporciona a la organización la máxima resiliencia frente a desastres regionales y actores malintencionados.

Monitorización y validación del sistema

Esta función son las herramientas y procesos mediante los cuales la empresa se asegura de que su sistema de administración de backup y su almacenamiento de backup funcionen correctamente, y de que la empresa sea capaz de ejecutar un proceso de recuperación cuando sea necesario.

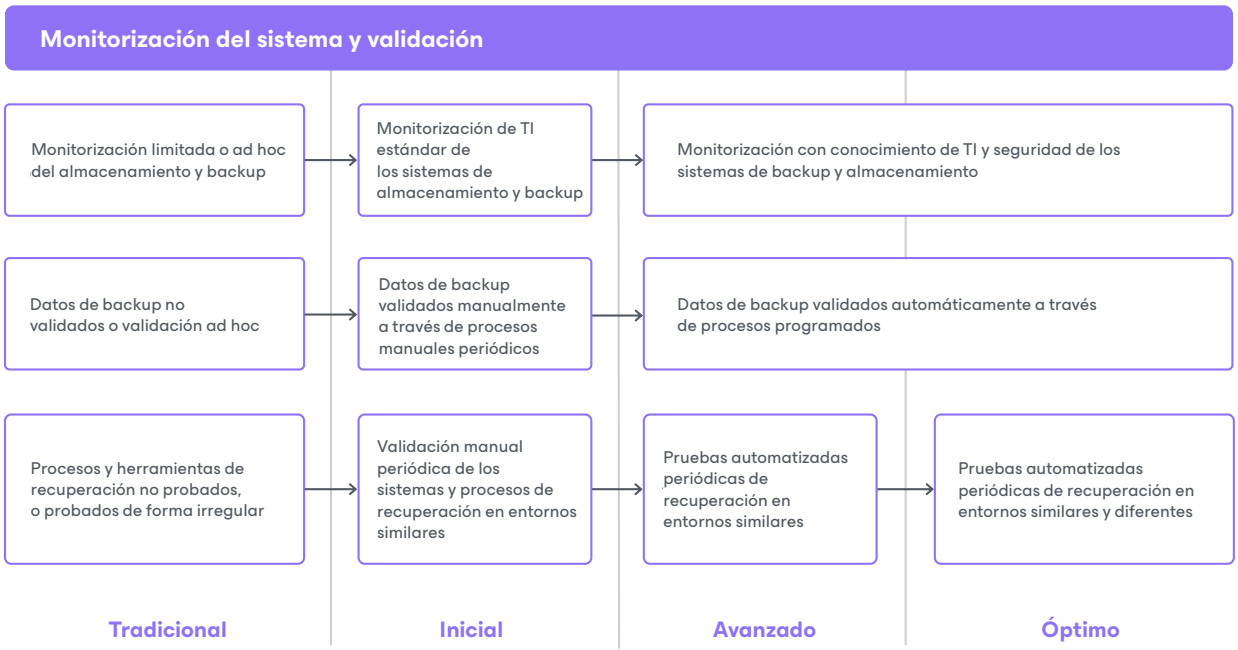


Figura 6 - Monitorización y validación del sistema: Modelo de Madurez

En el nivel de madurez **Tradicional**, la empresa solo realizará la monitorización básica de la infraestructura de backup y almacenamiento, lo que a menudo refleja una menor madurez general de las operaciones y la TI. Es posible que la organización no valide los datos de los que se ha hecho backup o que solo realice comprobaciones periódicas (es decir, manuales y poco frecuentes). Además, la empresa no probará de manera periódica las herramientas y los procesos de recuperación para que se entiendan bien, se documenten y se puedan repetir.

En el nivel **Inicial**, habrán adoptado un nivel estandarizado de monitorización operativa y de TI del sistema de backup y almacenamiento. También instituirán la validación periódica de los datos respaldados a través de procesos manuales. También habrán implementado una validación periódica (manual) de los procesos de recuperación para garantizar el conocimiento institucional y la familiaridad con los mismos.

En el nivel **Avanzado**, las organizaciones habrán implementado herramientas y procesos de monitorización de TI y seguridad para los sistemas de backup y almacenamiento. Además, validarán automáticamente los datos respaldados con comprobaciones programadas que informen y escalen cualquier resultado anómalo. Esto incluirá pruebas automatizadas de herramientas y procesos de recuperación en entornos similares al de producción.

En el nivel **Óptimo**, la organización habrá aumentado la sofisticación de sus pruebas de recuperación para probar su recuperación en entornos diferentes.

Resumen del modelo de madurez

En su conjunto, estas nuevas funciones definen un conjunto de funcionalidades y un conjunto esperado de competencias mapeadas en los cuatro niveles de madurez de Zero Trust. Proporcionan una hoja de ruta práctica y una guía para las empresas que buscan incorporar sus sistemas de backup y recuperación de datos a su iniciativa Zero Trust.

Conclusión

Zero Trust es una forma demostrablemente mejor de abordar la seguridad de la información y, como líderes de seguridad, tenemos la obligación de llevar esta estrategia a nuestras empresas. Las arquitecturas y los modelos de madurez actuales de Zero Trust son puntos de partida sólidos, pero están incompletos. En particular, los requisitos y enfoques de backup y recuperación de datos están ausentes en ellos.

Tradicionalmente, las empresas han tratado el backup y la recuperación como si estuvieran dentro del dominio de TI, pero la prevalencia del ransomware y la digitalización casi completa del negocio requieren que los líderes de seguridad amplíen su alcance para incluir esto.

En este white paper, hemos presentado el concepto de Resiliencia de datos Zero Trust, con un conjunto de principios básicos, una arquitectura de referencia y ampliaciones al Modelo de Madurez de Zero Trust. Creemos que al adoptar este enfoque de Resiliencia de datos Zero Trust, las empresas podrán seguir un rumbo claro y preciso hacia sistemas defensivos más sólidos, operaciones más eficientes y una recuperación más rápida. Los datos empresariales son demasiado importantes como para que no apliquemos las mejores prácticas de seguridad, y Zero Trust es la forma más eficaz de hacerlo.

Acerca de Veeam Software

Veeam®, el líder n.º 1 del mercado mundial en resiliencia de datos, cree que todas las empresas deberían ser capaces de recuperarse para avanzar después de una interrupción con la confianza y el control de todos sus datos cuando y donde los necesiten. Veeam llama a esto resiliencia radical, y estamos obsesionados en crear formas innovadoras de ayudar a nuestros clientes a conseguirlo. Las soluciones de Veeam están diseñadas específicamente para potenciar la resiliencia de datos al proporcionar backup de datos, recuperación de datos, libertad de datos, seguridad de datos e inteligencia de datos. Con Veeam, los líderes de TI y seguridad descansan tranquilos sabiendo que sus aplicaciones y datos están protegidos y siempre disponibles en sus entornos de nube, virtuales, físicos, SaaS y de Kubernetes. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550 000 clientes en todo el mundo, incluido el 74 % de las empresas de Global 2000, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia radical comienza con Veeam. Más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X @veeam.

Más información: veeam.com