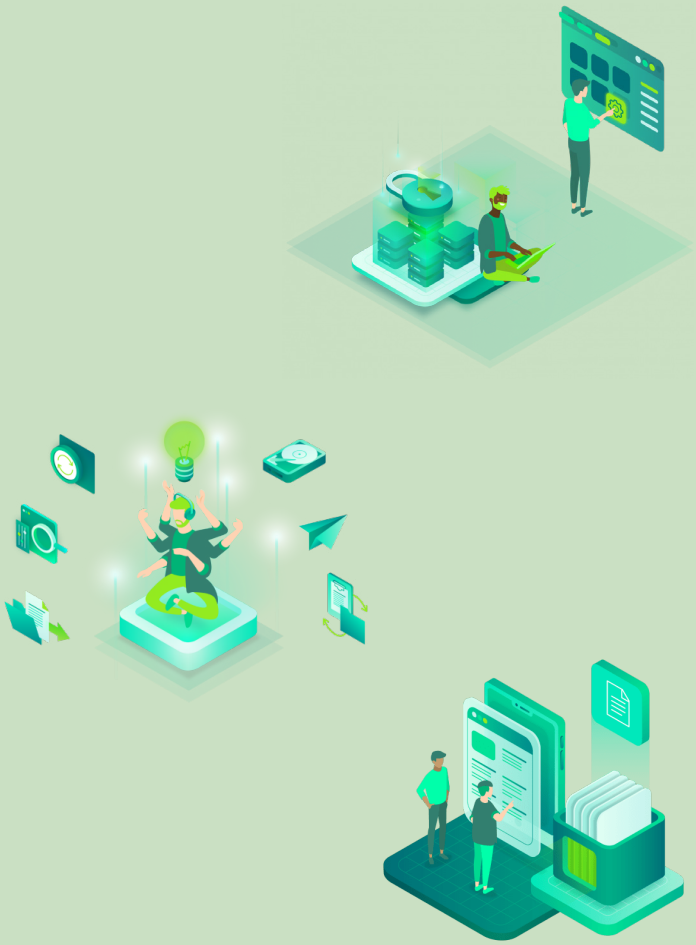
CCN-CERT

BP/34



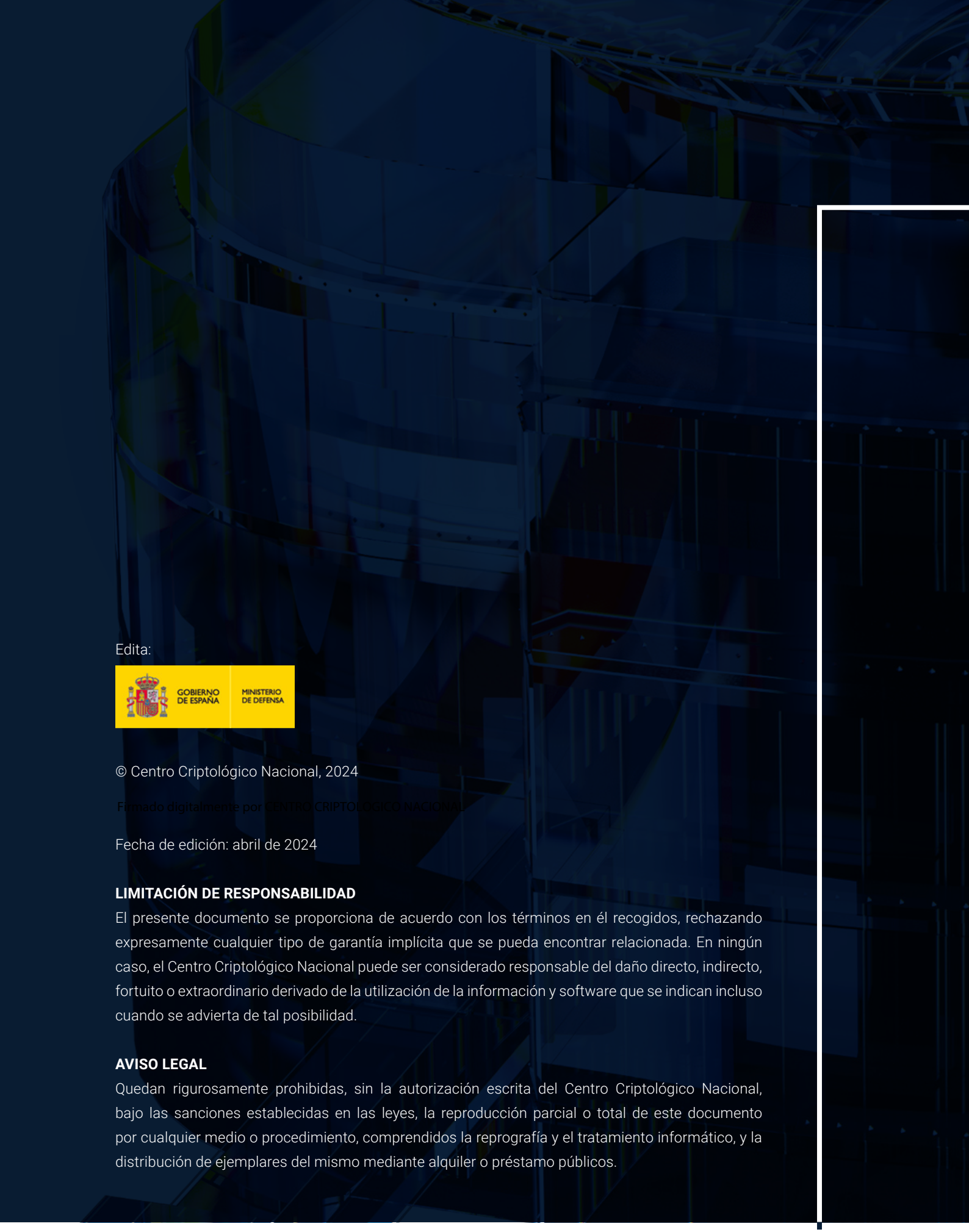
Recomendaciones de Seguridad sobre Veeam Data Platform

INFORME DE BUENAS PRÁCTICAS

ABRIL 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional



Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de edición: abril de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. Introducción

Veeam proporciona a las empresas y organizaciones una plataforma unificada para la protección de entornos de nube, virtuales, físicos, SaaS y Kubernetes.

Proporciona una plataforma unificada para la protección de entornos diversos, gestionada centralmente y adaptable a diferentes arquitecturas.

Los principales elementos que componen la solución son:

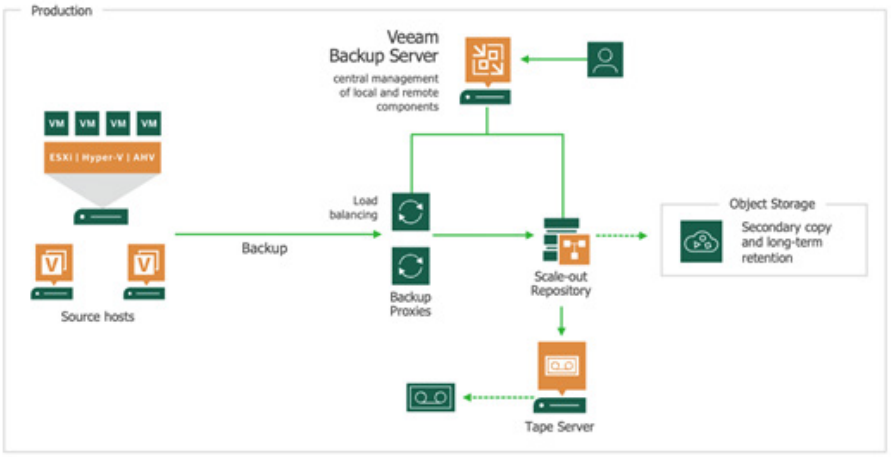
- **Veeam Backup Server:** es el elemento central que permite configurar y gestionar el resto de los componentes de la solución.
- **Veeam Backup Proxy:** la función principal del servidor proxy es leer los datos del entorno de producción y procesarlos para enviarlos al repositorio de backup.
- **Veeam Repository Server:** los repositorios se encargan de almacenar las imágenes de copia de seguridad y los metadatos.

Toda la información relativa a metadatos se encuentra autocontenida en el propio backup (en el repositorio local y también en la copia que se desborde en la nube), por lo que no se necesita ninguna base de datos de índices, volúmenes o deduplicación almacenada en el servidor de backup. Esto aporta ventajas en caso de recuperación frente a un desastre total o parcial del centro de datos local.

Es importante mencionar que, dependiendo de las necesidades o tamaño de la infraestructura, estos componentes se pueden instalar en un único equipo (all-in-one installation) o de forma desacoplada en distintos equipos.

1. Introducción

Una posible arquitectura a alto nivel de la solución podría ser la siguiente:



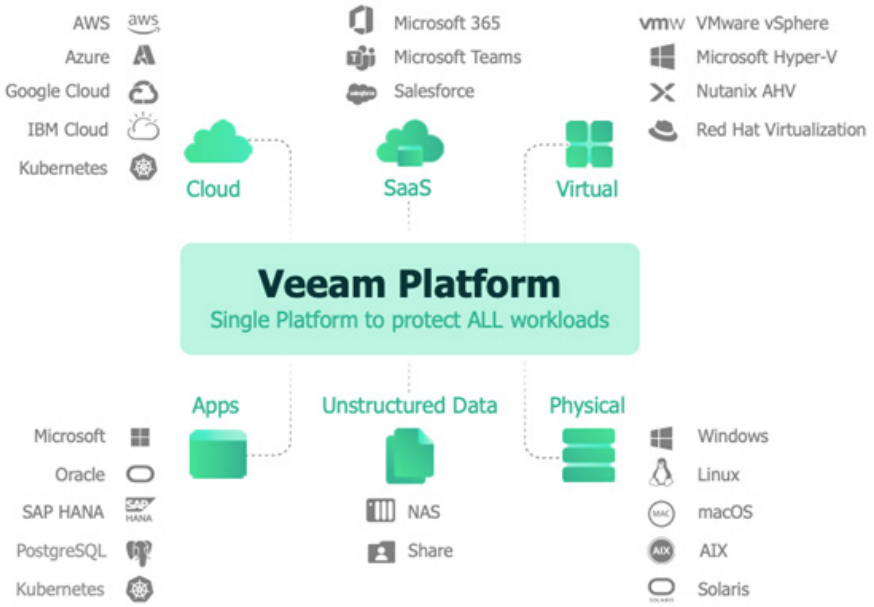
En el esquema se puede observar:

- Los múltiples orígenes de datos que Veeam soporta. Entornos virtualizados, servidores físicos, entornos de NAS o servidores de ficheros entre otros.
- En la parte central del proceso de copia se encuentran los "backup proxys", que se encargan de leer y procesar los datos de origen, enviándolos al repositorio de backup, comprimidos y deduplicados.
- En la parte derecha de la imagen se encuentra el repositorio de backup. Este habitualmente será local para dotar a la solución de un alto rendimiento tanto en la generación del backup como en procesos de restauración. Es posible replicar o extender el repositorio, ya sea localmente o en la nube, para poder seguir la típica regla de 3-2-1 que debería aplicar cualquier solución de backup.
- Opcionalmente es factible externalizar las copias a cinta, garantizando así la disposición de estas fuera de línea e incluso en distintas instalaciones.
- Todo ello gestionado de forma centralizada por el Veeam Server a través de una consola protegida con mecanismos de autenticación multifactor que ayudan a cumplir requerimientos técnicos y normativos.

2. Ransomware, resiliencia y seguridad

Veeam Data Platform es modular y extensible, lo que significa que puede ofrecer protección virtual y física en entornos locales, protección nativa en la nube en entornos AWS, Azure y Google Cloud, Kubernetes en cualquier lugar, así como protección SaaS para entornos Microsoft 365 y Salesforce.

Brinda protección completa para entornos virtuales, físicos, SaaS y Kubernetes, con opciones de copia de seguridad sin agentes y medidas avanzadas contra ransomware.



- **Cargas virtuales.** Veeam permite realizar una copia de seguridad de imagen, tanto a nivel de máquina virtual como de aplicación, sin la instalación de ningún tipo de agente, ni para la copia ni para la restauración.

  En el caso de bases de datos (Microsoft SQL Server, PostgreSQL u Oracle), Veeam permite también proteger los logs de transacciones de manera regular, sin instalación de agentes.

- **Cargas físicas.** Veeam permite la protección de equipos físicos Windows, Linux, MAC, AIX y Solaris mediante los "Veeam Agents". Para ello, es preciso instalar un único agente en el sistema que permite proteger el servidor de forma global (el sistema operativo, carpetas y aplicaciones).

  Los agentes se gestionarán de manera centralizada desde el servidor de Veeam y los datos viajan directamente del servidor al repositorio de backup y al igual que sucede con las cargas virtuales, para proteger los datos de la organización, todo el proceso de copia se encuentra cifrado de extremo a extremo (origen, red y destino).

- **Cargas NAS / Servidor de ficheros.** La funcionalidad NAS Backup se emplea para la protección de entornos de ficheros (NAS o File Servers Windows/Linux, físicos o virtuales).
  La copia de seguridad de los dispositivos NAS (SMB/CIFS y NFS) se realiza a través de la red local y los datos son procesados por los "File Proxies" que se encargarán de procesar los datos y enviarlos directamente a disco.

- **Cargas de contenedores basadas en Kubernetes.** K10 de Veeam ha sido diseñado especialmente para Kubernetes y proporciona a los equipos de operaciones un sistema fácil de usar, escalable y seguro para copias de seguridad y restauración, recuperación ante desastres y movilidad de aplicaciones de Kubernetes.

  Se integra de forma nativa en Kubernetes para descubrir automáticamente todos los componentes de la aplicación que se ejecutan en el clúster y tratar la aplicación como una unidad. Por otro lado, presenta soporte Multi-Tenancy con seguridad integrada, gestión multi-clúster y protección contra ransomware al soportar almacenamiento de objetos inmutables.

- **Cargas de nubes nativas.** Otra modalidad posible es la de realizar una copia de seguridad y recuperación modular y nativa de nube para proteger las cargas de trabajo específicas de AWS, Azure o Google Cloud.

2. Ransomware, resiliencia y seguridad

Los ataques por ransomware son actualmente una de las amenazas más graves y frecuentes para las organizaciones. Disponer de una defensa sólida, una estrategia robusta de protección de los datos y planes de recuperación agiles y probados son la mejor forma de protegerse ante este tipo de amenazas.

Las copias de seguridad, validadas y verificadas, son la última línea de defensa contra los ciberataques y pueden ser el factor decisivo para evitar un tiempo de inactividad considerable, la pérdida de datos y el impacto negativo en el negocio y la reputación de las organizaciones.

Es recomendable **a la hora de planificar las copias de seguridad, seguir la regla 3-2-1-1-0.** Esta es una mejora implementada por Veeam de la conocida regla 3-2-1.

Con la **regla 3-2-1-1-0**, la práctica sugerida es disponer de **(3) copias diferentes** de los datos, en **(2) tipos de medios** diferentes, **(1)** de los cuales se localice en **una ubicación externa** a la habitual, **(1)** de los cuales se encuentre **fuera de línea, aislado o inmutable,** y que cuente con **(0) errores** en las copias de seguridad, ya que han sido previamente probadas y verificadas automáticamente como recuperables.

Una **estrategia de ciberdefensa robusta y completa** siempre empieza por las copias de seguridad y éstas deben ser fiables, verificadas y probadas. Por otro lado, la **inmutabilidad es un paso clave** que impedirá a los ciberdelincuentes acceder a los datos de respaldo, cifrarlos o eliminarlos.

La inmutabilidad proporciona la **protección de un almacenamiento offline** de forma WORM (Write Once, Read Many), lo que hace que los datos de respaldo sean impenetrables a los ataques. Son posibles varias opciones de inmutabilidad en nube pública (AWS, Azure, Wasabi, etc.), así como repositorios S3 compatibles con "object lock" para la inmutabilidad en el entorno local, por no hablar también de las opciones de respaldo en cinta.

3. Buenas prácticas de seguridad en Veeam

3.1 Proteger

3.1.1 Proteger las copias de seguridad - la regla del 3 2 1 1 0

Una infraestructura de respaldo correctamente diseñada debe **incluir un mecanismo de protección de datos.** Este puede ser ofrecido por características tales como:

- "Appliances de deduplicación" mediante mecanismos propios como la inmutabilidad o las instantáneas protegidas.
- Almacenamiento de objetos, mediante Inmutabilidad.
- Dispositivos de cinta, con un "air gapping" físico.
- Mediante mecanismos WORM (Write Once, Read Many).

Se recomienda **proteger todas las retenciones mediante "air gap" o inmutabilidad.** Como el tiempo de permanencia de los atacantes es de aproximadamente un mes de media, es fundamental proteger al menos **cuatro (4) semanas de puntos de restauración** para mitigar el ataque.

Siguiendo **la regla 3-2-1-1-0** se crean múltiples capas de resistencia y seguridad. Los datos y las cargas de trabajo se harán inmutables (protección contra borrado y modificación), se almacenarán off-line (protección contra amenazas internas) y se dispondrá de un "air-gap" (protección contra amenazas internas y externas y otros desastres de continuidad de negocio, como incendios, inundaciones, terremotos, etc.)

Adicionalmente, es posible añadir lo que se denomina una **ruptura de protocolo**, para dificultar a los atacantes la destrucción de los datos. Consiste en utilizar diferentes tipos de repositorios, basados en diferentes tecnologías (bloque de disco, CIFS, NFS, S3, protocolos propietarios de dispositivos de deduplicación, etc.), entorpeciendo de este modo que las herramientas de ataque apunten a los datos.

3.1.2 Protección de la infraestructura de backup

Se recomienda proteger la infraestructura de Veeam aplicando **contramedidas como el "bastionado" o endurecimiento** de los componentes. Al menos la protección debe tener en consideración los siguientes:

- **Veeam Backup Server.**
- **Cuentas de Usuario.**
- **Repositorios de respaldo.**
- **Flujos de datos de respaldo.**

Debe considerarse que la solución de Backup es un **objetivo prioritario de los ataques a una infraestructura.** Su acceso debe ser muy restringido, y tanto este como su propio despliegue deben estar controlados en todo momento.

Los **proxies de copia de seguridad** deben considerarse un **objetivo para comprometer la información.** Durante el proceso de generación de la copia, los proxies obtienen del servidor de copia de seguridad las credenciales necesarias para acceder a los servidores de la infraestructura virtual. Un usuario con privilegios de administrador en un proxy de copia de seguridad puede interceptar las credenciales y utilizarlas para acceder a la infraestructura virtual.

3.1.3 Capacitación del personal

A través de acciones y formaciones de concienciación a los empleados, se incrementa de forma sensible la capacidad de estos para **detectar comportamientos extraños,** así como la concienciación de su papel fundamental en la protección de los servicios y datos de la organización.

Esto no es sólo aplicable al departamento de TI, sino a todos los usuarios de una organización, dado que todos ellos pueden ser **testigos de comportamientos sospechosos, o ser objeto de ingeniería social pudiendo potencialmente abrir una brecha de seguridad** si no disponen de la debida capacitación y concienciación en seguridad.

3.2 Detección de amenazas

3.2.1 Vigilancia

Para saber cuándo se está siendo atacado o se ha sufrido una brecha de seguridad, es vital tener **visibilidad de toda la ruta de flujo de datos.** Se debe poder diferenciar un "comportamiento anormal", de aquel que no lo es. Para ello, se recomienda supervisar las cuentas y la infraestructura de Veeam con el objeto de detectar actividades sospechosas.

Una de las medidas más efectivas es la colocación de **trampas virtuales,** como puede ser la creación de una cuenta de administrador no utilizada y con alarmas vinculadas a ella (por ejemplo, "Usuarios Honeypot"). Cuando se observe cualquier actividad en esa cuenta, se activará al instante una alerta.

Es importante recibir alertas lo antes posible para defenderse de otros ataques como virus, malware y ransomware. El mayor peligro de estos es la posibilidad de propagarse rápidamente a otros sistemas. **Disponer de vigilancia sobre, por ejemplo, la posible actividad de un ransomware es fundamental.**

3.2.2 Servidores honeypot

"Honeypot servers" o servidores señuelo con monitorización de autenticación pueden ayudar a detectar ataques dirigidos a la infraestructura Veeam. Estos señuelos deben ser visibles, y sus entradas DNS deberán ser comprensibles, como por ejemplo "vbrsrv01" o "vbrrepo", apareciendo, así como objetivos fáciles para el atacante.

Un señuelo adecuado podría incluir un repositorio falso, en el que se vigilaran de cerca los posibles cambios en los archivos de copia de seguridad.

3.2.3 Usuarios honeypot

"Honeypot users" o usuarios señuelo con monitorización de autenticación ayudan también a la detección de ataques dirigidos a la infraestructura Veeam. Como en el caso de los servidores señuelo, estos usuarios deben ser visibles y sus nombres muy comprensibles, como por ejemplo "VBRAdmin" o "BackupAdmin" para que sean considerados por el atacante como objetivos potencialmente asequibles.

Por supuesto, se deben **configurar estos usuarios para que su exposición y posible explotación maliciosa sea inútil,** por lo que su compromiso no tiene ningún efecto sobre la seguridad de la infraestructura de la organización.

3.2.4 Alarmas

"Veeam One" ofrece la posibilidad de monitorizar la posible actividad de ransomware a través de un conjunto de **alarmas predefinidas como "estado de inmutabilidad", "posible actividad de ransomware "o "seguimiento de cambios de inmutabilidad".**

Estas alarmas deben activarse tanto en el servidor de producción como en el "honeypot".

3.3 Estrategia de recuperación

Disponer de una estrategia de recuperación y saber cómo actuar cuando se produce un incidente es clave para minimizar el impacto de este y las pérdidas económicas asociadas. Lógicamente entre las recomendaciones fundamentales se encuentran la **realización de copias de seguridad de los datos, asegurando que un atacante no pueda acceder a ellas para borrarlas o alterarlas.**

En este sentido, copias externas (air-gap) o de sólo lectura en cualquier soporte son muy recomendables. Además, es necesario ser consciente de que en caso de denuncia ante las fuerzas de seguridad es muy probable que los activos sean precintados por entidades gubernamentales para su análisis o análisis forense y por lo tanto no se encontrarán disponibles para la recuperación. Es por ello recomendable **disponer de hardware de recuperación dedicado y mantener copias fuera de las instalaciones.**

Es también muy probable que la **conexión a Internet se deshabilite como método de expulsión del atacante** y/o evitar fugas de datos. Por lo tanto, puede que sea necesaria una forma alternativa de acceder a las copias de seguridad externas.

La preparación es la clave. En definitiva, haber probado la recuperación teniendo en consideración que habrá que realizar el reinicio únicamente desde archivos de copia de seguridad e infraestructuras que parten cero.

Otras recomendaciones a considerar son: t**ener el grupo de respuesta preparado,** conocer los activos a **priorizar en la recuperación**, así como utilizar de forma adecuada las herramientas de pruebas y automatización, como “Veeam SureBackup” o “Veeam Disaster Recovery Orchestrator”.

3.4 Roles y usuarios

El control del acceso a las herramientas de gestión es crucial para mantener una buena práctica de protección. En todos los casos se debe **utilizar el principio del mínimo privilegio.**

Un atacante que obtuviera acceso con privilegios elevados a los servidores de la infraestructura de respaldo puede obtener las

credenciales de las cuentas de usuario y **poner en peligro otros sistemas de su entorno** o aprovecharse de los procedimientos de recuperación.

Es por ello necesario asegurarse de que **todas las cuentas tienen un rol y permisos específicos y controlados.** Algunas recomendaciones en este sentido son:

- No utilizar cuentas de usuario para el acceso con privilegios administrativos.
- Proporcionar a cada administrador de Veeam su propia cuenta específica con privilegios administrativos, para facilitar la trazabilidad, la adición y eliminación.
- Eliminar el rol por defecto "Veeam Backup Administrator" del grupo de Administradores Locales.
- Otorgar sólo el acceso necesario para el trabajo a realizar durante el tiempo que sea de necesidad (JIT).
- Limitar de forma estricta los usuarios que pueden iniciar sesión mediante "Veeam Console".
- Añadir autenticación de doble factor a los activos de gran valor.
- Monitorizar las cuentas en busca de actividades sospechosas.

3.4.1 Cuentas no predecibles

Muchas empresas y organizaciones siguen como buena práctica el uso de cuentas dedicadas para que los administradores ejecuten tareas privilegiadas independientes a su cuenta de usuario, la cual les permite realizar tareas básicas de oficina.

Estas cuentas a menudo llevan el prefijo "adm_", lo que puede ser útil, pero ayuda a los atacantes a identificar las cuentas con privilegios. **Es recomendable utilizar las cuentas "adm_" sólo para los usuarios "honeypot" y elegir otra estrategia de denominación para las cuentas de administración reales.**

Las redes sociales también pueden ayudar en la identificación de un posible propietario de una cuenta privilegiada dentro de una empresa u organismo. Se recomienda por ello evitar el uso del nombre del usuario, añadiendo de este modo complejidad a la identificación de cuentas privilegiadas.

3.4.2 Política de gestión de contraseñas

Se recomienda utilizar una **política de gestión de contraseñas funcional pero inteligente**. Imponer el uso de contraseñas seguras en toda la infraestructura es imprescindible, dificultando a los atacantes el descubrimiento de contraseñas o el descifrado de hashes para obtener acceso no autorizado a sistemas críticos.

Es también necesario **verificar que se han modificado regularmente las cuentas y contraseñas** por defecto en todos los activos. En el caso de las cuentas administrativas, es imprescindible **añadir la autenticación de dos factores (2FA)** para una mayor protección de la infraestructura.

Se recomienda verificar que la herramienta de contraseñas y la base de datos se encuentren disponibles en un **sitio de recuperación** para poder disponer de ellas en caso de que se produzca un desastre o incidente crítico. Es necesario que una copia de seguridad reciente de la herramienta de contraseñas y de la base de datos debe residir en un medio protegido "air-gap", como un DVD, CD-ROM o cinta. La más crucial es la contraseña de "Veeam Repository" que permite la restauración a partir de los archivos de copia de seguridad.

El acceso a los sistemas de producción desde la infraestructura de respaldo puede basarse en **"Group Managed Service Accounts" (gMSA)** para facilitar la consecución de un buen nivel de seguridad, ya que en ese caso **se establecen y rotan automáticamente contraseñas complejas.** "Group Managed Service Accounts" puede utilizarse con "Veeam Backup and Replication" desde la versión 12.

3.4.3 Política de bloqueo

Es recomendable el uso de una **política de bloqueo** que complemente una política inteligente de gestión de contraseñas. Las cuentas se bloquearán después de un limitado número de intentos incorrectos. Esto puede **detener los ataques de adivinación de contraseñas.**

Es necesario considerar que esta política **puede también bloquear el sistema de copia de seguridad y replicación** durante un tiempo. Para las cuentas de servicio, a veces es preferible generar una alarma rápidamente en lugar de bloquear las cuentas. De esta forma se obtiene visibilidad sobre comportamientos sospechosos hacia los datos o la infraestructura.

3.4.4 Permisos requeridos

Como se ha indicado anteriormente, se recomienda seguir el **principio de menor nivel de privilegio,** es decir, proporcionar los permisos mínimos necesarios para que las cuentas de usuario o de servicio funcionen.

3.5 Protocolos de autenticación

Se recomienda elegir **algoritmos de cifrado fuertes para SSH**. Para comunicar con los servidores Linux desplegados como parte de la infraestructura de respaldo, "Veeam Backup & Replication" utiliza SSH. Para el túnel SSH se recomienda utilizar un **algoritmo de cifrado robusto y probado,** con una longitud de clave suficiente. Es necesario asegurar que las claves privadas se guardan en un lugar seguro y no pueden ser descubiertas por terceros.

Desde "Veeam Backup & Replication v12", es posible una arquitectura sólo Kerberos, así que **se recomienda deshabilitar la autenticación NTLM siempre que sea posible.**

3.6 Cifrado

3.6.1 En reposo

Se debe utilizar el **cifrado integrado de Veeam Backup & Replication** para proteger los datos de las copias de seguridad. Además, para configurar dicho cifrado, se recomienda seguir las prácticas recomendadas de cifrado en reposo:

- Contraseñas seguras que sean difíciles de descifrar o adivinar.
- Guardar las contraseñas en un lugar seguro.
- Cambiar las contraseñas de los trabajos cifrados con regularidad.

3.6.2 En tránsito

Los datos de copia de seguridad y réplica pueden ser interceptados en tránsito, cuando se comunican desde el origen al destino a través de una red. Para proteger el canal de comunicación del tráfico de copia de seguridad, es necesario tener en cuenta estas directrices:

- **Aislar el tráfico de copia de seguridad.** Utilizar una red segmentada para transportar datos entre los componentes de la infraestructura de copia de seguridad: servidor de copia de seguridad, proxies de copia de seguridad, repositorios, etc.
- **Cifrar el tráfico de red.** Por defecto, "Veeam Backup & Replication" cifra el tráfico de red que viaja entre redes públicas, pero se recomienda activar el cifrado del tráfico en redes privadas para garantizar la comunicación segura de datos confidenciales dentro de los límites de la misma red.

3.7 Bastionado

El bastionado consiste en proteger la infraestructura contra los ataques reduciendo la superficie de ataque y minimizando el riesgo al máximo posible.

Una de las principales medidas para el fortalecimiento es la **eliminación de todos los programas de software y utilidades no esenciales** de los componentes de Veeam desplegados. Aunque estos componentes pueden ofrecer funciones útiles para el administrador, si proporcionan acceso adicional al sistema deben eliminarse durante el proceso de fortalecimiento.

Configurar la vigilancia y registro de eventos de lo que ocurre en la infraestructura forma parte del refuerzo de esta. Se recomienda verificar que es posible detectar cuándo puede producirse o se ha producido un ataque y a continuación confirmar que los registros y rastros se guardan para que fuerzas de seguridad y especialistas en seguridad puedan hacer uso de ellos en caso de necesidad.

Dificultar y por lo tanto ralentizar la operativa de los atacantes es siempre un objetivo a considerar. De este modo **nombrar los servidores de infraestructura de respaldo utilizando nombres no relacionados** con el mismo es una buena estrategia. Evitar nombres que contengan acrónimos como "bkp", "pxy", "repo", "vbr" o cualquier denominación que pueda facilitar la identificación de los componentes de la infraestructura de respaldo forma parte de esta estrategia.

3.7.1 Segmentación

Una buena estrategia es diseñar un marco de **defensa en profundidad que incluya todas las capas.** Para ello, se deben identificar los datos más valiosos y construir capas de defensa a su alrededor para proteger su disponibilidad, integridad y confidencialidad.

Una zona es un área que tiene una característica particular, un propósito, un uso y/o está sujeta a restricciones particulares. En lugar de una protección global con el mismo nivel, se asocian sistemas e información a zonas específicas y aquellos sistemas que están sujetos al cumplimiento normativo pueden agruparse en subzonas para limitar el alcance de la comprobación del cumplimiento y, por tanto, reducir los costes y el tiempo necesarios para completar largos procesos de auditoría.

Es necesario pensar en la importancia de los datos y sistemas de esa zona concreta y en quién debe tener acceso a ellos. **Sólo se debe permitir la comunicación entre sistemas de zonas adyacentes.** Una clasificación de datos común para una zona se refiere a los requisitos de disponibilidad compartida, confidencialidad, integridad, controles de acceso, auditoría, registro y supervisión.

Estas características y requisitos comunes conducen intrínsecamente a cierto nivel de aislamiento, pero este aislamiento se produce no sólo entre zonas, sino también dentro de las zonas denominadas subzonas.

La superficie de ataque de los datos y sistemas dentro de una zona puede **reducirse significativamente exponiendo un número limitado de servicios** a través del perímetro de la zona e implementando estrictos **controles de acceso,** limitando este a grupos específicos de usuarios. Un posible atacante tendría que acceder a todas las zonas exteriores antes de llegar a la zona restringida donde se almacenan los datos críticos, lo que reduce la probabilidad de robo o mutilación de datos. Además, se incrementa la disponibilidad de estos sistemas críticos.

Es posible utilizar un **modelo de zonas como modelo de defensa estratégica** que divide los diferentes componentes de Veeam en zonas separadas. Se recomienda tener en cuenta las **siguientes reglas durante el diseño:**

- **Seguro por diseño.**
- **Identificar qué es importante, añadir seguridad y clasificación.**
- **Conocer los vectores de ataque y las posibles formas de protección.**
- **Usar el principio del menor privilegio.**
- **Disponer una visión de costes y beneficios.**

No existe una fórmula exacta que resuelva todas las necesidades de seguridad a la vez. Hay muchas formas de conseguir el objetivo. No hay que creer que un entorno es seguro porque se han seguido todas las buenas prácticas, en ese caso se tendría una falsa sensación de protección.

Se deben analizar las necesidades de la organización y elegir la mejor manera de satisfacerlas, teniendo en cuenta el presupuesto, los riesgos (vectores de ataque) y los posibles resultados (cuál sería el daño).

3.7.2 Capas entre zonas

Cada una de las zonas adyacentes puede valorarse a través de **las siete (7) capas del modelo de ciberseguridad:**

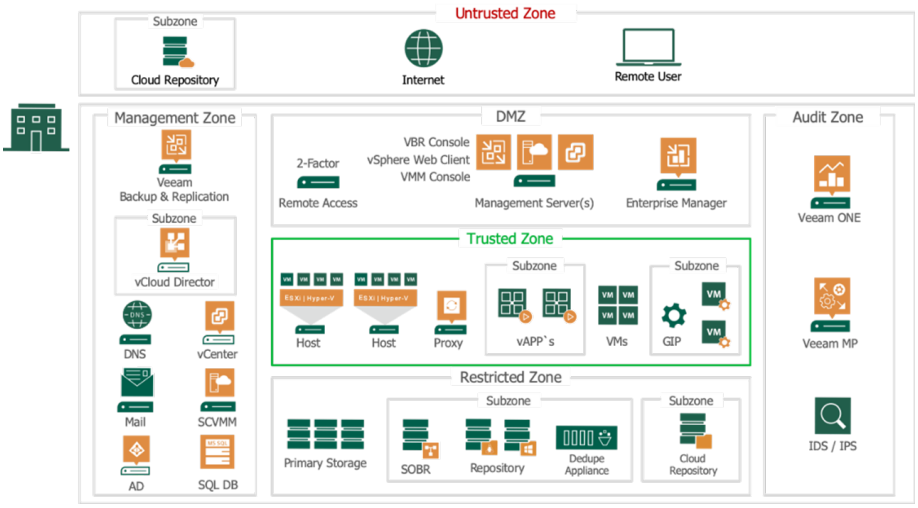
- **Capa humana:** formación, acceso físico…
- **Perímetro:** firewalls, filtros de Spam, detección/prevención de Intrusiones…
- **Red:** diseño y topología seguros, VLAN, cortafuegos multicapa/ conmutadores…
- **“Endpoint”:** Antivirus, Software Firewalls, “Breach Detection Agents” …
- **Aplicaciones:** parches, actualizaciones, ...
- **Datos:** cifrado en reposo y en tránsito.
- **Misión Crítica:** respaldo, respuesta y plan de recuperación.

3.7.3 Ejemplos usando zonas

Hoy en día **la mayoría de las amenazas provienen del interior** por lo que se recomienda dividir la infraestructura en zonas para proporcionar una mejor visibilidad de las partes de mayor importancia. Para reforzar la seguridad de los componentes de la infraestructura de "Veeam Availability", estos se colocan en varias zonas lógicas.

Uno de los vectores de ataque más buscados será **obtener acceso a las cuentas y componentes de gestión.** En "Veeam Backup & Replication" hay tres (3) componentes de gestión disponibles.

- Consola de "Veeam Backup & Replication", también referida como "Console".
- Servidor de "Veeam Backup & Replication", es el componente central que orquesta todos los diferentes trabajos y ordena el movimiento de los datos a través de la infraestructura.
- "Veeam Backup Enterprise Manager", que federa múltiples "Backup Servers" en una única consola de gestión.



3.7.3.1 Zona no Fiable (Untrusted Zone)

Para mantener un equilibrio entre la seguridad y la eficiencia operativa, **no es deseable instalar "Veeam Backup & Replication Console" en ningún sistema fuera de la infraestructura** de la organización.

Se recomienda **desplegar un cortafuegos en el perímetro** entre la zona no confiable y la zona DMZ. En el cortafuegos y/o en el servidor dedicado del "gateway RDS", añadir **autenticación de doble factor** para que los administradores remotos puedan acceder al "gateway RDS".

Se debe **restringir y denegar la asignación de unidades, impresoras, portapapeles,** etc. en el "gateway RDS" para proteger la infraestructura contra la descarga de contenidos o archivos desde cualquier equipo remoto.

3.7.3.2 DMZ

La DMZ alberga **sistemas que requieren exposición a la zona no fiable.** Esta zona permite el acceso entre los sistemas en la DMZ y la Zona de Gestión.

La consola de "Veeam Backup & Replication" es un componente del lado del cliente que proporciona acceso al servidor de respaldo. La consola permite que varios operadores y administradores de respaldo inicien sesión en "Veeam Backup & Replication" simultáneamente y realicen todo tipo de operaciones de protección de datos y recuperación ante desastres como si trabajaran en el servidor de respaldo.

Se puede instalar la consola de "Veeam Backup & Replication" en un **servidor de gestión central que esté situado en la zona DMZ**, protegiéndolo con **autenticación de doble factor (2FA).** También es posible instalar otras herramientas de infraestructura en este servidor de gestión como, por ejemplo, Microsoft VMM Console y/o VMware vSphere Client para gestionar la implementación de hipervisor.

En caso de ser necesario, "Veeam Enterprise Manager" también se puede instalar en la zona DMZ, ya que sirve como **portal de autoservicio para grupos de usuarios específicos** de la organización.

3.7.3.3 Zona de Gestión (Management Zone)

En la zona de gestión, se colocan **servicios de infraestructura como DNS, Active Directory y SMTP.** Pero también, el servidor VMware vCenter y/o Microsoft System Center Virtual Machine Manager (SCVMM).

De los componentes de Veeam, el servidor o servidores "Veeam Backup & Replication" estarán en esta zona de gestión. El "Veeam Backup Server" orquestará todos los trabajos y actualizará todos los componentes de Veeam en las diferentes zonas desde una ubicación central.

El **servidor de base de datos Microsoft SQL**, necesario para alojar la base de datos de copia de seguridad de Veeam y la base de datos de copia de seguridad de "Veeam Enterprise", **debe colocarse en esta zona si está dedicado sólo a Veeam.** Es una buena práctica **utilizar un servidor SQL dedicado** que aloje las diferentes instancias SQL para los componentes de la infraestructura y **un servidor SQL diferente para las instancias SQL de los procesos empresariales.**

El servidor "Veeam Backup & Replication" es un usuario intensivo del servidor SQL, por lo que colocar el servidor de base de datos SQL cerca aumenta la eficiencia operativa. VMware vCloud Director forma parte de una subzona dentro de la zona de gestión y controla las vAPP que se ejecutan en subzonas dentro de la zona de confianza.

La zona de gestión **requiere un acceso seguro y controlado a Internet para descargar licencias y actualizaciones** de los distintos componentes de la infraestructura. Se recomienda encarecidamente utilizar un **proxy de Internet o un proxy inverso** situado en la DMZ como pasarela controlada a Internet.

Todos los tipos de repositorios en la nube deben colocarse en **subzonas dentro de la zona No Confiable.** Los datos de la organización están saliendo de los límites de seguridad, así que es necesario **asegurarse de que, como precaución adicional, los datos hacia estos repositorios en la nube se cifran** durante el transporte y cuando se almacenan en el repositorio en la nube.

El servidor "Veeam Backup & Replication" se comunicará con el servicio Cloud Gateway para el transporte de los datos hacia el Cloud Provider, Azure Proxy o AWS deployment.

3.7.3.4 Zona de Confianza (Trusted Zone)

La zona de confianza estará poblada de **hosts de hipervisor** como VMware ESXi y/o hosts Microsoft Hyper-V. Todos los componentes de la zona de confianza necesitarán acceso a distintos servicios de la zona de gestión. Los servidores "Veeam Proxy", que son los que mueven los datos, forman parte de la zona de confianza.

"Veeam Proxies" pueden realizar copias de seguridad de las máquinas virtuales sin tener acceso a los propios sistemas operativos invitados. Si se realizan copias de seguridad o réplicas de máquinas virtuales en ejecución, se pueden habilitar las opciones de procesamiento de invitados.

Las opciones de procesamiento de invitados son tareas avanzadas que requieren que "Veeam Backup & Replication" se comunique con el sistema operativo invitado de la máquina virtual. Cuando las máquinas virtuales están separadas en subzonas, se pueden desplegar y aprovechar del "Veeam Guest Interaction Proxy" (GIP), en la subzona de confianza, que tendrá acceso seguro y desplegará el tiempo de ejecución necesario en la máquina virtual para las tareas de procesamiento de invitados.

En el caso de que diferentes unidades de negocio o clientes se ejecuten en la zona de confianza, se debería pensar en ejecutarlas en subzonas de esta. Pero hay que tener en consideración que **los diseños demasiado complejos pueden ser contraproducentes** y suministrar una sensación errónea de seguridad.

Las vAPPs de VMware vCloud Director también forman parte de la Zona de Confianza y normalmente se dividirían en subzonas por unidad de negocio o inquilino. Veeam puede capturar vApps enteras y configuraciones de vCloud Director dentro de los trabajos de backup.

3.7.3.5 Zona Restringida (Restricted Zone)

El almacenamiento primario, donde residen los datos de producción y las máquinas virtuales deben situarse en esta zona restringida, pero también deben hacerlo otros componentes que almacenan datos.

Esta zona nunca debe ser accesible por ningún usuario directamente. Sólo se encuentra disponible para los componentes de la infraestructura virtual y los servidores de aplicaciones y administradores con derechos estrictos.

Además, el "Veeam Scale Out Backup Repository" (SOBR), el "Simple Repository", los dispositivos de deduplicación o el "Cloud Repository" cuando se utilizan en combinación con "Veeam Cloud Connect for Enterprise (VCC-E)" deben formar parte de esta zona. Para las organizaciones que utilizan VCC-E es posible definir repositorios en la nube sobre el SOBR o como repositorios en la nube definidos por separado en una subzona de Zona Restringida.

3.7.3.6 Zona de Auditoría (Audit Zone)

La visibilidad es clave para proteger, detectar y contener las amenazas de forma temprana. En esta zona se sitúan las soluciones de monitorización como "Veeam ONE" y/o "Veeam Management Pack" en combinación con Microsoft System Center. Asimismo, los sistemas IDS e IPS deben situarse en esta zona de auditoría.

3.7.4 Reducción de la superficie de ataque

3.7.4.1 Acceso a la consola

La consola de "Veeam Backup & Replication" es un componente del lado del cliente que proporciona acceso al servidor de respaldo. La consola permite que varios operadores y administradores de respaldo inicien sesión en "Veeam Backup & Replication" simultáneamente y realicen todo tipo de operaciones de protección de datos y recuperación ante desastres como si trabajaran en el servidor de respaldo.

Es preferible **instalar "Veeam Backup & Replication Console" en un servidor de gestión central situado en una zona de red segura y protegido con autenticación de doble factor (2FA)** en lugar de múltiples instalaciones de la consola en los escritorios locales de los administradores de respaldo y recuperación. Se recomienda **aplicar siempre MFA** al autenticarse en la propia "VBCR" (compatible a partir de v12).

El acceso a "Veeam Backup & Replication Server" debe limitarse a la consola de "Veeam Backup & Replication", cualquier protocolo de acceso remoto debe ser deshabilitado.

3.7.4.2 Desinstalar la consola del servidor Backup

El "Backup & Replication Console" debe **eliminarse del "Veeam Backup & Replication Server" siempre que sea posible.** La consola se instala localmente en el servidor de copia de seguridad de forma predeterminada.

La Consola no puede eliminarse a través del instalador o utilizando Agregar/Quitar en Microsoft Windows. Es necesario abrir un símbolo del sistema "cmd" con acceso administrativo. En el símbolo del sistema escriba: wmic product list brief > installed.txt esto creará un documento de texto con todos los productos instalados y sus respectivos códigos de producto.

Para desinstalar "Veeam Backup & Replication Console", se requiere desinstalar primero todos los "Veeam Explorers":

- **"Veeam Explorer for Microsoft Exchange".**
- **"Veeam Explorer for Microsoft SharePoint".**
- **"Veeam Explorer for Microsoft Active Directory".**
- **"Veeam Explorer for Microsoft SQL".**
- **"Veeam Explorer for Oracle".**

Se pueden desinstalar estos componentes utilizando: *msiexec /x {ProductCode}*

Ejemplo para desinstalar "Veeam Backup & Replication console": msiexec /x {D0BCF408-A05D-45AA-A982-5ACC74ADFD8A}

NOTA: La desinstalación de la consola de "Veeam Backup and Replication" elimina el módulo de PowerShell e imposibilita el uso de los "cmdlets" de PowerShell de "Veeam Backup" en el servidor de copia de seguridad. Esto puede afectar a los scripts de automatización o productos que dependen de PowerShell para interactuar con "Veeam Backup and Replication", por ejemplo "Veeam Recovery Orchestrator" (antes "Veeam Disaster Recovery Orchestrator").

3.7.4.3 Protección de la base de datos de Veeam Backup & Replication

La base de datos de configuración de copia de seguridad y replicación almacena credenciales para conectarse a servidores virtuales y a otros sistemas de la infraestructura de copia de seguridad y replicación.

Todas las contraseñas almacenadas en la base de datos se encuentran cifradas. Sin embargo, **un usuario con privilegios de administrador en el servidor de copia de seguridad puede descifrar las contraseñas,** lo que representa una amenaza potencial.

Para proteger la base de datos de configuración de "Backup & Replication", se siguen estas directrices:

- **Restringir el acceso de los usuarios a la base de datos.** Se debe garantizar que solo los usuarios autorizados pueden acceder al servidor de copia de seguridad y al servidor que aloja la base de datos de configuración de "Veeam Backup & Replication" (si la base de datos se ejecuta en un servidor remoto).

- **Cifrar los datos en las copias de seguridad de configuración.** Se recomienda activar el cifrado de datos en las copias de seguridad de la configuración para proteger los datos almacenados en la base de datos de configuración. Es necesario tener en cuenta que las cuentas de usuario y las contraseñas no se almacenan en las copias de seguridad de configuración cuando el cifrado no está activado.

3.7.4.4 Eliminación de componentes no utilizados

Eliminar todos los programas de software y aplicaciones innecesarias de los componentes de Veeam desplegados. Aunque estos programas pueden ofrecer funciones útiles para el administrador, también **proporcionan accesos no deseados** ("puertas traseras") al sistema, deben eliminarse durante el proceso de fortalecimiento.

Software adicional como navegadores Web, Java, Adobe Reader y programas similares deben ser desinstalados. En general, se recomienda **eliminar todas las funcionalidades ajenas al sistema operativo** o a los componentes activos de Veeam. Esto hará que mantener un nivel de parches actualizado sea mucho más efectivo.

3.7.4.5 Eliminación de servicios no utilizados

Desactivar el servicio "Veeam vPower NFS" en cada componente en el que no tenga previsto utilizar las siguientes funciones de Veeam: "SureBackup", "Instant Recovery" u operaciones de recuperación a nivel de archivos (FLR) de otro S.O.

Eliminar el proxy predeterminado y el rol de repositorio predeterminado del servidor VBR si no se tiene previsto su uso. De igual modo, cuando no se utilice Enterprise Manager, se recomienda también su **desinstalación y eliminación del entorno.**

3.7.4.6 Parches y actualizaciones

Aplicar parches de seguridad a los sistemas operativos, para el software y el firmware de los componentes de Veeam es fundamental. La mayoría de los ataques tienen éxito porque ya hay software vulnerable en uso que no está alineado con los niveles de parches actuales.

Por lo tanto, es muy importante **verificar que todos los componentes de software y hardware en los que se ejecutan componentes de Veeam se encuentren actualizados.** Una de las causas más comunes del robo de credenciales son las actualizaciones del sistema operativo invitado y el uso de protocolos de autenticación obsoletos.

Para mitigar los riesgos, se pueden seguir las siguientes directrices:

- Rastrear las Vulnerabilidades y Exposiciones Comunes (CVE) de los sistemas.
- Verificar que los Sistemas Operativos de los servidores de infraestructura se actualizan regularmente.
- Instalar las últimas actualizaciones y parches en los servidores de infraestructura de respaldo para minimizar el riesgo de explotación de vulnerabilidades del sistema operativo por parte de los atacantes.

Se puede optar por aislar el servidor "Veeam Backup and Replication" de Internet. En ese caso es necesario proceder con **actualizaciones offline.** Para ello se descargan las actualizaciones desde otro equipo, se copian los binarios en el servidor VBR y se aplican las actualizaciones descargadas.

En aquellos casos en donde "Veeam Backup and Replication Server" puede acceder a Internet, es necesario **restringir estrictamente el acceso a los servidores de actualización de aplicaciones y sistemas operativos,** eliminando de nuevo cualquier herramienta y navegador, evitando con ello la instalación/descarga de posibles piezas de código dañinas. Por supuesto, **nunca se debe exponer "Veeam Backup and Replication Server" a Internet.**

3.7.4.7 Puertos

Es mejor no **utilizar puertos oscuros u otros mecanismos** para intentar ocultar los puertos y protocolos en uso de Veeam, aunque esto pueda parecer una buena opción. En la práctica esto suele dificultar la gestión de la infraestructura, lo que abre otras posibilidades a los atacantes. La ocultación no siempre es sinónimo de seguridad.

Se han desarrollado dos (2) herramientas para facilitar la identificación de puertos entre los componentes de Veeam:

- **"Veeam Network Port Mapping Tool".**
- **"Ports List Finder".**

Se recomienda **aplicar las reglas de cortafuegos adecuadas** para restringir las comunicaciones de red a las necesidades mínimas de las aplicaciones.

3.7.5 Grupo de trabajo o dominio

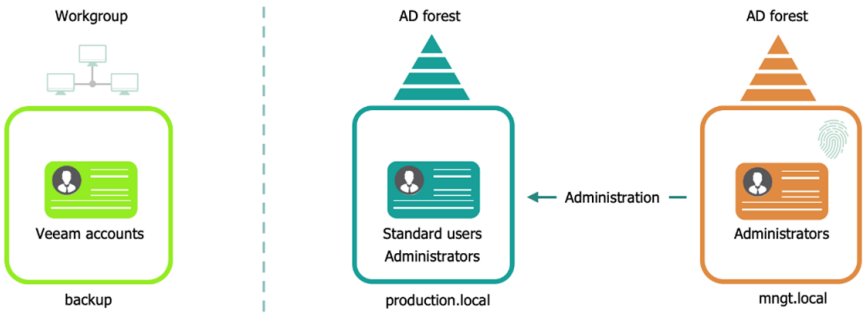
Microsoft Active Directory es el corazón de la infraestructura TI de casi todas las organizaciones. Al configurar la infraestructura de "Veeam Availability", es necesario tener en consideración el principio de que **un sistema de protección de datos no debe depender en modo alguno del entorno que debe proteger.**

Esto se debe a que cuando el entorno de producción falle junto con los controladores de dominio, afectará a la capacidad para realizar restauraciones reales debido a la dependencia del servidor de copia de seguridad de esos controladores de dominio para la autenticación de la consola de copia de seguridad, DNS para la resolución de nombres, etc.

A la hora de proteger las cuentas administrativas y la instalación de la infraestructura de Veeam, se dispone de **varias opciones, desde la más segura hasta la menos segura:**

- Agregar los componentes de Veeam a un dominio de administración que resida en un bosque de Active Directory independiente y proteger las cuentas administrativas con mecanismos de autenticación de dos factores (2FA).
- Agregar los componentes de Veeam a un grupo de trabajo separado y colocar los componentes en una red separada cuando proceda.

Añadir los componentes de Veeam al dominio de producción, pero verificando que las cuentas con privilegios administrativos están protegidas con autenticación de dos factores (2FA).



3.7.5.1 Buenas prácticas

Para el despliegue más seguro **se recomienda añadir los componentes de Veeam a un dominio de administración** que resida en un bosque de Active Directory separado y proteger las cuentas administrativas con mecanismos de autenticación de dos factores (2FA).

De este modo, la infraestructura de disponibilidad de Veeam no depende del entorno que debe proteger.

3.7.5.2 Grupo de trabajo de Windows

Cuando se utiliza un **grupo de trabajo, es necesario tener todo cuidadosamente documentado por razones de gestión y cumplimiento.** Cada sistema necesita ser configurado independientemente con una política de seguridad local, así como una gestión de usuarios, asignación de permisos, etc. específicos para cada caso.

Teniendo varios servidores Veeam y múltiples usuarios, esto podría llegar a ser **extremadamente dificultoso en grandes entornos.** No se puede utilizar autenticación Kerberos con un servidor de grupo de trabajo, en su lugar **se utilizará NLTM, lo cual puede suponer en sí mismo un riesgo añadido.**

Un grupo de trabajo es más difícil de defender contra amenazas procedentes del interior, como puede ser un empleado descontento, dado que puede utilizar cuentas locales en los servidores del grupo de trabajo, no siendo posible desactivar una sola cuenta AD bloqueando a ese empleado específico de la infraestructura crítica. Además, **es más**

difícil demostrar por necesidades de cumplimiento normativo que los sistemas son seguros y se utilizan correctamente. Una configuración de grupo de trabajo es una buena solución para entornos de un tamaño limitado.

Ventajas

- Rápido y fácil de configurar.
- Separa las cuentas de Veeam de las cuentas privilegiadas del dominio (ayuda contra los keyloggers y la violación del dominio de producción).
- No depende del entorno que debe proteger.
- No requiere servidores de infraestructura, como Domain Controllers, NTP o DNS.

Inconvenientes

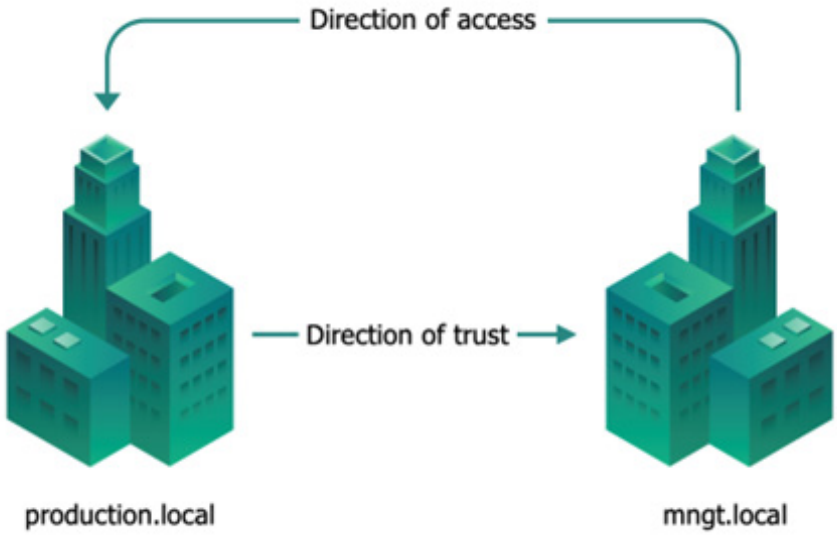
- Gran sobrecarga de gestión en entornos grandes.
- No hay comunicación Kerberos al iniciar sesión en un servidor independiente (grupo de trabajo), sólo NTLM.
- Es más difícil cumplir la normativa, hacer comprobaciones de cumplimiento y demostrar que se cumple con los marcos de referencia adoptados.
- No es posible utilizar el sistema de autenticación gMSA para la interacción de las copias de seguridad de los SO invitados.

3.7.5.3 Dominio de gestión

Aunque este enfoque añade un bosque a un entorno de Directorio Activo, el coste y la complejidad se ven limitados por el diseño fijo, la pequeña huella de hardware/software y el reducido número de usuarios. Permitir la gestión central de políticas, derechos de usuario y permisos facilita la gestión. También permite desactivar con un solo clic una única cuenta de AD cuando es necesario enfrentarse a una amenaza interna como la mencionada anteriormente.

Configurar un bosque independiente con un dominio de gestión es la mejor opción para entornos grandes. También se puede añadir la **autenticación multifactor** en el dominio para proteger aún más las cuentas administrativas, bloqueando los ataques del tipo "Man in the Middle" y los "keyloggers".

Los bosques de confianza (Forest trusts) ayudan a gestionar una infraestructura segmentada de Servicios de dominio de Active Directory (AD DS) y a admitir el acceso a recursos y otros objetos en varios bosques. Además, son útiles para las organizaciones que buscan una solución de autonomía administrativa ya que se pueden vincular dos (2) bosques diferentes para formar una relación de confianza transitiva unidireccional o bidireccional. Un bosque de confianza permite a los administradores conectar dos (2) bosques AD DS con una única relación de confianza para proporcionar una experiencia de autenticación y autorización sin fisuras en los bosques.



Si se crea una relación de confianza unidireccional entre dos bosques, los miembros del "trusted forest" utilizan los recursos situados en el "trusting forest" y la confianza opera únicamente en una dirección.

3.7.6 Worm Storage con Veeam Hardened Repository

"Veeam Hardened Repository" es una solución de almacenamiento tipo "WORM" que protege contra cambios no deseados en los archivos de respaldo. Está disponible desde la versión 11 y admite las siguientes características:

- **Inmutabilidad:** cuando se agrega un repositorio reforzado, se especifica el período de tiempo en el que los archivos de copia de seguridad deben ser inmutables. Durante este período, los archivos almacenados en este repositorio no se pueden modificar ni eliminar.
- **Credenciales de un solo uso:** credenciales que se utilizan en una única ocasión para desplegar Veeam Data Mover, o el servicio de transporte, mientras se añade el servidor Linux a la infraestructura de backup. Estas credenciales no se almacenan en la infraestructura de copia de seguridad. Incluso si el servidor de Veeam Backup & Replication se ve comprometido, el atacante no puede obtener las credenciales y conectarse al repositorio reforzado.confidenciales dentro de los límites de la misma red.

Como recordatorio o complemento de la guía del usuario, se recomiendan las siguientes acciones para crear un repositorio reforzado:

- **Desplegar el repositorio de Veeam utilizando credenciales de un solo uso:** Veeam no almacenará la cuenta root del repositorio, manteniendo los archivos de respaldo seguros si el servidor "Veeam Backup" se ve comprometido. No hay que olvidar eliminar el usuario del grupo "sudoers" tras la instalación.
- **Desactivar SSH después de la implementación:** la conexión SSH sólo es necesaria para el despliegue o actualización de "Veeam Data Mover". Una vez desplegado Veeam, es posible desactivar SSH para mejorar la seguridad. Si se mantiene activo, se debería de habilitar la autenticación multifactor para su uso.
- **IPMI:** cualquier herramienta de gestión, como ILO o DRAC puede ser utilizada para acceder al repositorio, e incluso para borrar los discos duros. Se recomienda encarecidamente desconectar estas herramientas de la red cuando no se utilicen.
- **NTP:** la gestión del tiempo es crucial cuando se habla de inmutabilidad. No es aconsejable utilizar servidores NTP públicos, ya que ello implicaría la exposición en Internet del servidor de repositorio. Utilizar un servidor NTP propio es una opción, pero puede suponer un riesgo de seguridad en caso de que un atacante tome el control del mismo.

El uso del reloj CMOS interno es una opción aconsejable, pero la contrapartida es la necesidad de comprobar regularmente y ajustar manualmente la hora del sistema. Además, una diferencia horaria entre el repositorio y el servidor de copia de seguridad haría más complejo el análisis forense de los registros. Como segunda opción aconsejable e interesante es utilizar un dongle DCF77 (o equivalente local) con el paquete XNTP para sincronizar el repositorio en señal de onda larga.

3.7.7 Procesado de aplicaciones

"Application Aware Processing" requiere que la infraestructura "Veeam Backup and Replication" inicie sesión en los servidores de producción para interactuar con los sistemas operativos y las aplicaciones.

Aunque permite que las aplicaciones y el sistema de archivos sean coherentes en el momento de la copia de seguridad, puede considerarse un riesgo, ya que cualquier credencial proporcionada se almacenará en la base de datos de configuración de "Veeam Backup and Replication".

Las soluciones alternativas serían:

- Realizar los respaldos sin "Application Processing", es decir, realizar respaldos tolerables a fallos.
- Utilizar gMSA (Group Managed Service Accounts) en VBR v12 o posterior.
- Utilizar agentes para realizar los respaldos.

NOTA: Los elementos de aplicación aún pueden restaurarse de forma granular desde una copia de seguridad que no tenga en cuenta la aplicación a través de los exploradores. Para ello, se inicia una restauración de "Guest file" y, desde el explorador, se fuerza una "Application Item restore".

3.7.7.1 gMSA

Aunque no sea totalmente seguro, si se considera la necesidad de delegar la gestión de contraseñas a Microsoft gMSA se debe tener en consideración que **el servidor VBR tendrá entonces que formar parte del dominio.**

3.7.7.2 Active Directory Backup

Un respaldo consistente de Active Directory requiere credenciales "Built-in Administrator" en el huésped. Para evitar almacenar estas credenciales en la base de datos de Veeam, **es una buena práctica realizar copias de seguridad de los servidores de Active Directory utilizando un agente no gestionado** contra un repositorio de Veeam.

De esta forma, la cuenta de Administrador permanecerá protegida y la restauración de elementos de Active Directory mediante el explorador solicitará el inicio de sesión adecuado en el momento de la restauración.

3.7.7.3 Ubicación del Guest Interaction Proxy

Los "Guest interaction proxies" permiten interactuar con máquinas virtuales Microsoft Windows en zonas de menor seguridad sin exponer por ello el servidor de copia de seguridad en estas zonas.

El uso del "Guest interaction Proxy" con invitados limitará drásticamente la exposición del servidor de copia de seguridad y replicación de Veeam. Los puertos necesarios para el procesamiento de la interacción con invitados se encuentran disponibles en la guía del usuario.

3.7.7.4 Ubicación de la Console for Explorers

El despliegue de "Veeam Console" en zonas aisladas será de gran ayuda a la hora de restaurar elementos invitados, ya que **permitirá operar sin necesidad de abrir el rango de puertos dinámicos RPC de Microsoft** desde la zona de gestión a la zona aislada. La consola puede desplegarse en el "Guest interaction Proxy" que ya debería estar en esa zona.

3.7.7.5 Credenciales para restauraciones

En el momento de la restauración, cuando se utilizan los "Veeam Explorers", la autenticación contra el servidor de destino se realiza utilizando las credenciales de interacción de invitados configuradas en el trabajo de copia de seguridad. Si se cambian las credenciales en la configuración del trabajo, cambiará la cuenta utilizada en el momento de la restauración.

La eliminación de la configuración de interacción de invitados incurrirá en la introducción interactiva de credenciales en el momento de la restauración.

4. Decálogo de recomendaciones

A continuación, se indican diez recomendaciones de seguridad en el uso de Veeam Data Platform.

Decálogo de recomendaciones para Veeam Data Platform

1. Se recomienda implementar la **seguridad desde el inicio del diseño** del entorno. Así como, una infraestructura de respaldo correctamente diseñada.

2. Se recomienda **proteger las copias de seguridad** y respaldo, la infraestructura, así como capacitar al personal de la organización.

3. Se recomienda trazar una estrategia que permita **monitorizar alertas, usuarios, servidores** y demás **elementos críticos** que formen parte del sistema.

4. Se recomienda contar con un **plan de recuperación**, así como formar al personal necesario para llevarlo a cabo, esto reducirá el tiempo de actuación en caso de incidente.

5. Se recomienda desplegar **una política de Control de Acceso** a los componentes de gestión utilizando el principio del mínimo privilegio. Imponer la contención para evitar que los atacantes se muevan con demasiada facilidad (cambiar las reglas del juego al atacante).

6. Se recomienda crear una **política robusta de contraseñas** e implementar una **política de bloqueo** ante intentos fallidos de inicio de sesión evitando los ataques de fuerza bruta.

7. Se recomienda elegir **algoritmos de cifrado fuertes** para los accesos remotos a la infraestructura de respaldo.

8. Se recomienda para el cifrado de datos **habilitar cifrado tanto en tránsito como en reposo** para evitar brechas y lecturas indeseadas.

9. Se recomienda **reducir la superficie de ataque** eliminando todos los programas de software y utilidades no esenciales de los componentes de Veeam desplegados.

10. Se recomienda la **segmentación en diversas áreas**, reducir la superficie de exposición eliminando complementos o funcionalidades que no sean de necesidad, contar con copias de seguridad inmutables, así como gestionar de forma adecuada otros productos o soluciones que se utilicen junto con Veeam.

Anexo A. Medidas de seguridad ENS y controles de seguridad

En la siguiente tabla se vinculan diferentes medidas de seguridad del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad con las soluciones de Veeam Backup, poniéndose de manifiesto su aplicabilidad, así como referencia al apartado correspondiente de esta misma guía, donde se justifica:

Medida del ENS	Justificación de la aplicabilidad	Apartado en esta guía
Copias de seguridad [mp.info.6]	El objetivo de las soluciones de Veeam Backup es precisamente realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente **[mp.info.6.1]**. Permiten asimismo determinar la frecuencia de las copias, almacenar los backups en el propio lugar y/o en otros lugares y establecer controles para limitar el acceso autorizado a las copias de respaldo **[mp.info.6.2]**. Estas soluciones permiten, asimismo, la realización de pruebas de recuperación **[mp.info.6.r1.1]** y el almacenamiento de una de las copias de forma separada en un lugar diferente, de modo que un potencial incidente no pueda afectar simultáneamente ni a la información original, ni a la copia **[mp.info.6.r2.]**.	1. Introducción. 3.3 Estrategia de recuperación.
Identificación [op.acc.1] **Requisitos de acceso [op.acc.2]**	La gestión de cuentas se apoyará en la del dominio donde se implante la solución Veeam backup. Se emplean credenciales de un solo uso suministradas por el usuario de forma interactiva en el momento de la instalación inicial y al instalar actualizaciones del producto. Nunca se almacenan en la base de datos de configuración.	3.4 Roles y usuarios. 3.7.6 Worm Storage con Veeam Hardened Repository.

Medida del ENS	Justificación de la aplicabilidad	Apartado en esta guía
Mecanismo de autenticación [op.acc.5], [op.acc.6]	Todo el uso del protocolo SSH se ha encapsulado en un protocolo de transporte ampliado. Como resultado, la conectividad SSH sólo es necesaria en el momento de la implementación inicial y al instalar actualizaciones del producto. Esto permite a los clientes proteger SSH con autenticación multifactor interactiva (MFA) interactiva o incluso desactivar por completo el servidor SSH para proteger su repositorio, incluso de futuras vulnerabilidades de día cero. Desde "Veeam Backup & Replication v12", es posible una arquitectura sólo Kerberos, recomendándose deshabilitar la autenticación NTLM siempre que sea posible.	3.5 Protocolos de autenticación.
Plan de continuidad [op.cont.2]	Se recomienda que las copias de seguridad a nivel de imagen sean inmutables durante el tiempo especificado en la política de retención, de al menos cuatro (4) semanas, siguiendo un esquema GFS (Grand father, Father, Son). Esta funcionalidad utiliza la función nativa de inmutabilidad de archivos de Linux.	3.1.1 Protección de las copias de seguridad.
Criptografía [mp.si.2]	Se dispone del cifrado integrado de 'Veeam Backup & Replication' para proteger los datos en reposo de las copias de seguridad **[mp.si.2.r2.1].** Los módulos de cifrado están basados en FIPS.	3.6.1 Cifrado en reposo.
Separación de flujos de información en la red [mp.com.4]	Para aislar el tráfico de copia de seguridad se recomienda utilizar una red segmentada entre los componentes principales de la infraestructura de copia de seguridad: servidor de copia de seguridad, proxies de copia de seguridad, repositorios de copia, etc. **[mp.com.4.1]** Por defecto, "Veeam Backup & Replication" cifra el tráfico de red que viaja entre redes públicas, pero se recomienda activar el cifrado del tráfico también en redes privadas para garantizar la comunicación segura en la red interna. **[mp.com.2.r5.1]**	3.6.2 Cifrado en tránsito.
Registro de la actividad [op.exp.8]	Las soluciones de Veeam backup pueden añadir entradas en el registro de eventos del sistema para una mejor visibilidad para los usuarios que realizan una supervisión basada en dicho registro **[op.ep.8.1]**	3.7 bastionado. 3.7.1 segmentación.
Dimensionamiento / gestión de la capacidad [op.pl.4]	El empleo de repositorios de respaldo escalables mediante Scale-Out Backup Repositories (SOBR), facilita el gestionar la capacidad disponible para las copias de respaldo. **[op.pl.4.2], [op.pl.4.r1.2]**	

Anexo B. Lista de comprobación

Elemento	Comprobación	Resultado
REGLA 3-2-1-1-0		
3 copias	¿Hay 3 copias diferentes de los datos?	Si/No/Parcialmente/No sabe
2 medios	¿Las copias están alojadas en dos medios diferentes?	Si/No/Parcialmente/No sabe
1 offsite	¿Hay una copia fuera del sitio principal?	Si/No/Parcialmente/No sabe
1 inmutable / separada	¿Una copia es inmutable o está separada?	Si/No/Parcialmente/No sabe
0 errores	¿Se prueban periódicamente las copias de seguridad para garantizar que se puedan restaurar?	Si/No/Parcialmente/No sabe
DETECCIÓN DE AMENAZAS		
EDR-XDR	¿Se implementa un EDR o XDR para detectar amenazas?	Si/No/Parcialmente/No sabe
Honeypots	¿Se han implementado señuelos?	Si/No/Parcialmente/No sabe
VeeamOne	¿Veeam One está implementado y monitorizando las amenazas?	Si/No/Parcialmente/No sabe
ESTRATEGIA DE RECUPERACIÓN		
Existencia de estrategia de recuperación	¿Existe una estrategia de recuperación?	Si/No/Parcialmente/No sabe
Prueba de estrategia de recuperación	¿Se prueba periódicamente la estrategia de recuperación?	Si/No/Parcialmente/No sabe
Infraestructura de recuperación dedicada	¿Existe una infraestructura de recuperación dedicada?	Si/No/Parcialmente/No sabe
ROLES Y USUARIOS		
Cuentas anónimas	¿Los nombres de las cuentas contienen referencias a sus funciones?	Si/No/Parcialmente/No sabe
Política de cambio de contraseña	¿Se cambian las contraseñas periódicamente?	Si/No/Parcialmente/No sabe

Anexo B. Lista de comprobación

Elemento	Comprobación	Resultado
Política de bloqueo	¿Se desconectan los usuarios después de un período de inactividad determinado?	Si/No/Parcialmente/No sabe
Control de acceso basado en roles	¿Solo se puede acceder a la infraestructura de respaldo mediante cuentas de respaldo?	Si/No/Parcialmente/No sabe
Cuentas señuelo	¿Hay cuentas de señuelo visibles que sean monitorizadas?	Si/No/Parcialmente/No sabe
Multi Factor authentication	¿Se utiliza MFA para iniciar sesión en la infraestructura de respaldo?	Si/No/Parcialmente/No sabe
CIFRADO		
En reposo	¿Los datos están cifrados en los repositorios?	Si/No/Parcialmente/No sabe
En tránsito	¿Los datos están cifrados en tránsito?	Si/No/Parcialmente/No sabe
FORTIFICACIÓN		
Segmentación específica	¿La infraestructura de respaldo se encuentra en segmentos específicos?	Si/No/Parcialmente/No sabe
MFA	¿Está habilitada MFA en el segmento de infraestructura de respaldo?	Si/No/Parcialmente/No sabe
Veeam DB	¿Está restringido el acceso a la base de datos de Veeam?	Si/No/Parcialmente/No sabe
Consola	¿Se desinstala la consola del servidor VBR?	Si/No/Parcialmente/No sabe
Limpieza de servidores de infraestructura de respaldo	¿Se han limpiado los servidores de todas las funciones/componentes innecesarios?	Si/No/Parcialmente/No sabe
Parches y actualizaciones	¿Los servidores están parcheados/actualizados periódicamente?	Si/No/Parcialmente/No sabe
Gestión remota	¿Están deshabilitadas/desinstaladas las herramientas de administración remota?	Si/No/Parcialmente/No sabe
Inmutabilidad	¿El repositorio es inmutable?	Si/No/Parcialmente/No sabe
Fortificación	¿Está reforzado el repositorio?	Si/No/Parcialmente/No sabe
PROCESAMIENTO DE SOLICITUDES		
Credenciales del controlador de dominio	¿La cuenta de administrador del dominio está almacenada en Veeam?	Si/No/Parcialmente/No sabe
gMSA	¿Se utiliza gMSA para la interacción con los invitados?	Si/No/Parcialmente/No sabe

Anexo C. Glosario

Término	Descripción
AES-256	Algoritmo de cifrado
Air gap	Medida de seguridad para aislar un objeto de la red
API	Interfaz de programación de aplicaciones
Appliance	Elemento software o hardware que ha sido diseñado para proporcionar un recurso de computación específico
Backup	Copia de seguridad o respaldo
Baremetal	Servidor físico dedicado
Bastionado	El fortalecimiento o "bastionado" consiste en proteger la infraestructura contra los ataques reduciendo la superficie de ataque y eliminando así el mayor número posible de riesgos.
CCTV	Circuito Cerrado de Televisión
CIFS	Protocolo de transferencia de ficheros
Cloud	Conjunto de servidores remotos conectados a internet que ofrecen un servicio o propósito
Cluster	Conjunto de nodos de una infraestructura de kubernetes
CMOS	Complementary Metal Oxide Semiconductor, semiconductor complementario de óxido metálico), también llamada batería de tipo botón, en la placa base ayuda al BIOS o UEFI a almacenar los ajustes de configuración de hardware
Configmaps	Fichero de datos clave-valor
CPU (Central Processing Unit)	Unidad central de procesamiento
Criptoprocesadores	Microprocesador optimizado para realizar operaciones criptográficas
Deduplicar	Proceso informático de eliminación de datos duplicados
DMZ	Zona Desmilitarizada o DMZ es un área de la infraestructura en la que se exponen los servicios a redes inseguras como internet

Anexo C. Glosario

Término	Descripción
DNS (Domain Name System)	Servicio que traduce nombres de dominio en direcciones IP o viceversa
Dongle	Un adaptador o llave -del inglés dongle- es un pequeño dispositivo, que se conecta a otro dispositivo para aportar una función adicional.
DR (Disaster Recovery)	Proceso definido para recuperar datos ante la interrupción de un sistema
Failback	Capacidad de transferencia del entorno reparado al entorno original tras el fallo
Failover	Capacidad de un sistema para seguir funcionando en caso de fallo
Forest	Conjunto de dominios de Microsoft Windows
GDPR (General Data Protection Regulation)	Reglamento General de Protección de Datos
GPO (Group Policy Object)	Directiva de grupo, objeto de directorio activo que asigna una directiva o valor de configuración
Honeypot	Señuelo empleado para visualizar posibles ataques
IDS	Sistema de detección de intrusiones
IPS	Sistema de prevención de intrusiones
Kerberos	Protocolo de autenticación
keyloggers	Software malicioso que registra lo que se introduce en el teclado
Kubernetes	Plataforma de contenedores de código abierto
LAN	Red de área local
Multi-Tenant	Arquitectura de software que permite a una sola instancia servir a varios clientes
Namespace	Espacio de trabajo / espacio de nombres
NAS (Network Attached Storage)	Tecnología de almacenamiento conectado a la red
NDMP	Protocolo de gestión de datos en red
NFS	Protocolo de sistema de ficheros en red

Anexo C. Glosario

Término	Descripción
NTLM	Conjunto de protocolos de autenticación de Microsoft
NTP	Protocolo de sincronización de relojes
Object Storage	Almacenamiento basado en objetos
OIDC	Protocolo de autenticación
RBAC (Role-Based Access Control)	Control de acceso basado en roles
RPC	Programa de llamada a procedimiento remoto
RPO	Objetivo de punto de recuperación
RTO	Objetivo de tiempo de recuperación
SaaS	Software como servicio (Software as a service)
SAI	Sistema de Alimentación Ininterrumpida
Secret	Fichero de datos confidencial
SMB	Protocolo de transferencia de ficheros
SSH	Secure Shell es un protocolo de administración remota
Token	Identificador de validación
WAN	Red de área extensa
Workgroup	Grupo de trabajo de Microsoft Windows
WORM (Write Once, Read Many)	Método de copia de seguridad de una sola escritura y varias lecturas

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT
centro criptológico nacional

VEEAM

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es