Descripción del modelo de responsabilidad compartida

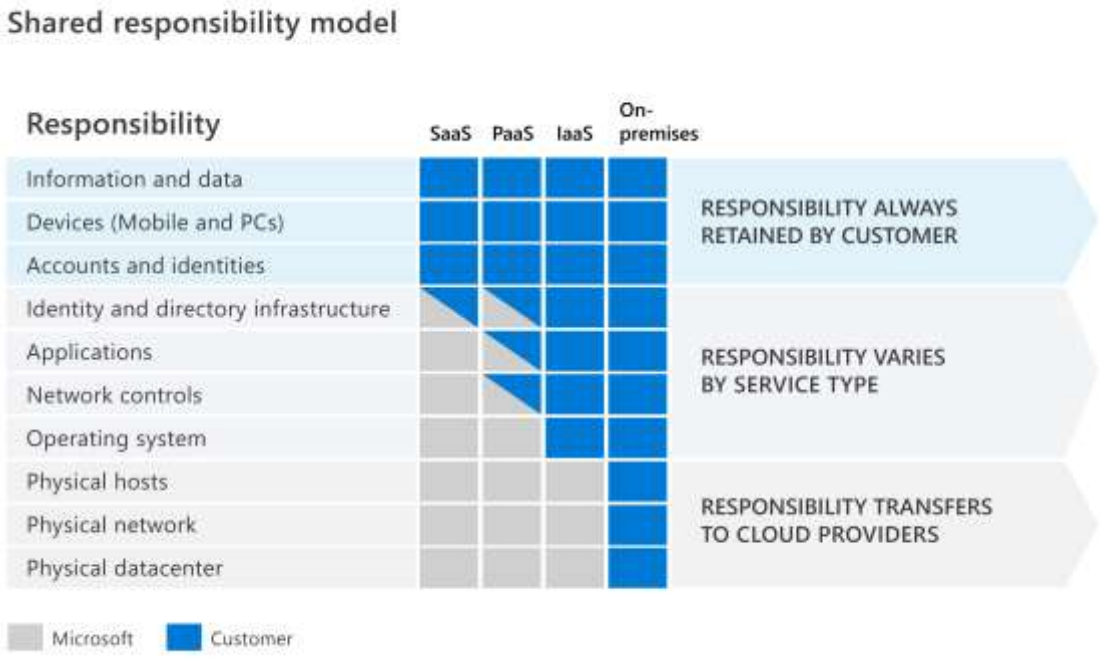
En organizaciones que solo ejecutan hardware y software local, la organización es un 100 % responsable de la implementación de la seguridad y el cumplimiento. Con los servicios basados en la nube, esa responsabilidad se comparte entre el cliente y el proveedor de la nube.

El *modelo de responsabilidad compartida* identifica qué tareas de seguridad administra el proveedor de la nube y qué tareas de seguridad administra usted como cliente. Igualmente, las responsabilidades varían en función de dónde se hospede la carga de trabajo:

- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)
- Infraestructura como servicio (IaaS)
- Centro de datos local

El modelo de responsabilidad compartida hace que las responsabilidades resulten claras. Cuando las organizaciones realizan migraciones a la nube, algunas responsabilidades se transfieren al proveedor de la nube y otras a la organización del cliente.

En el diagrama siguiente se muestran las áreas de responsabilidad entre el cliente y el proveedor de la nube, en función de dónde se encuentran los datos.



- **Centros de datos locales**. En un centro de datos local, usted es el responsable de todo, desde la seguridad física hasta el cifrado de la información confidencial.

- **Infraestructura como servicio (IaaS)**. De todos los servicios en la nube, IaaS requiere que el cliente en la nube se encargue de la mayor parte de la administración. Con IaaS, se usa la infraestructura informática del proveedor de la nube. El cliente en la nube no es responsable de los componentes físicos, como los equipos y la red, ni de la seguridad física del centro de datos. Sin embargo, el cliente en la nube sigue siendo responsable de los componentes de software, como los sistemas operativos, los controles de red, las aplicaciones y la protección de datos.
- **Plataforma como servicio (PaaS)**. PaaS proporciona un entorno para compilar, probar e implementar aplicaciones de software. El objetivo de PaaS es ayudarle a crear una aplicación rápidamente sin tener que administrar la infraestructura subyacente. Con PaaS, el proveedor de la nube administra el hardware y los sistemas operativos, y el cliente es responsable de las aplicaciones y los datos.
- **Software como servicio (SaaS)**. El proveedor en la nube se encarga de hospedar y administrar SaaS para el cliente. Normalmente, esto se licencia a través de una suscripción mensual o anual. Microsoft 365, Skype y Dynamics CRM Online son ejemplos del software de SaaS. El cliente en la nube solo debe administrar el mínimo de SaaS. Asimismo, el proveedor de la nube es responsable de administrar todo, excepto los datos, los dispositivos, las cuentas y las identidades.

En cuanto a todos los tipos de implementación en la nube, usted es el propietario de sus datos e identidades como cliente de la nube. Asimismo, es responsable de proteger la seguridad de los datos, las identidades y los recursos locales.

En resumen, las responsabilidades que siempre retiene la organización del cliente incluyen:

- La información y los datos.
- Los dispositivos (móviles y equipos).
- Las cuentas e identidades.

La ventaja del modelo de responsabilidad compartida es que las organizaciones tienen claras sus responsabilidades y las del proveedor de la nube.

Descripción de la defensa en profundidad

La defensa en profundidad usa un enfoque por capas para la seguridad, en lugar de depender de un solo perímetro. Una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque. Cada capa proporciona protección de modo que, si se infringe una de ellas, una capa posterior impedirá que un atacante obtenga acceso no autorizado a los datos.

Los niveles de seguridad de ejemplo pueden incluir:

- La seguridad física, como limitar el acceso a un centro de datos solo al personal autorizado.

- Controles de seguridad de identidad y acceso, como la autenticación multifactor o el acceso basado en condiciones, para controlar el acceso a la infraestructura y el control de cambios.
- La seguridad perimetral de la red corporativa incluye la protección frente a ataques de denegación de servicio distribuido (DDoS) para filtrar los ataques a gran escala antes de que puedan causar una denegación de servicio para los usuarios.
- Seguridad de red, como la segmentación de red y los controles de acceso a la red, para limitar la comunicación entre los recursos.
- Seguridad de capa de proceso, como la protección del acceso a las máquinas virtuales, ya sea de forma local o en la nube, cerrando determinados puertos.
- Seguridad de capa de aplicación, que garantiza que las aplicaciones sean seguras y estén libres de vulnerabilidades de seguridad.
- Seguridad de capa de datos que incluye controles para administrar el acceso a los datos empresariales y de clientes, y el cifrado para proteger los datos.

Confidencialidad, integridad, disponibilidad (CIA)

Como se ha descrito anteriormente, una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque. Todos los distintos mecanismos

(tecnologías, procesos y formación) son elementos de una estrategia de ciberseguridad, cuyos objetivos incluyen garantizar la confidencialidad, la integridad y la disponibilidad, a los que se suele hacer referencia como CIA, por sus siglas en inglés.

- La confidencialidad se refiere a la necesidad de conservar datos confidenciales, como información de clientes, contraseñas o datos financieros. Puede cifrar los datos para mantener la confidencialidad, pero también debe mantener la confidencialidad de las claves de cifrado. La confidencialidad es la parte más visible de la seguridad; gracias a ella, podemos ver claramente la necesidad de mantener la confidencialidad de los datos privados, las claves, las contraseñas y otros secretos.
- La integridad indica la necesidad de mantener los datos o mensajes correctos. Cuando envíe un mensaje de correo electrónico, probablemente quiera asegurarse de que el mensaje recibido sea el mismo que el mensaje enviado. Al almacenar datos en una base de datos, quiere asegurarse también de que los datos que recupera son los mismos que los datos almacenados. El cifrado de datos hace que este proceso sea confidencial, pero debe ser capaz de descifrarlo para obtener el mismo contenido que antes del cifrado. La integridad consiste en tener la confianza de que los datos no se han alterado ni modificado.
- La disponibilidad se refiere a poner los datos a disposición de los usuarios cuando los necesiten. Es importante para la organización mantener seguros los datos de los clientes, pero al mismo tiempo también debe estar disponible para los empleados que trabajan con los clientes. Aunque puede ser más seguro almacenar los datos en un formato cifrado, los empleados necesitan obtener acceso a los datos descifrados.

Aunque los objetivos de una estrategia de ciberseguridad son preservar la confidencialidad, la integridad y la disponibilidad de sistemas, redes, aplicaciones y datos, los ciberdelincuentes pretenden interrumpir estos objetivos. La cartera de Microsoft incluye las soluciones y tecnologías para permitir a las organizaciones cumplir el triple objetivo CIA.

Descripción del modelo de Confianza cero

La confianza cero presupone que todo está en una red abierta y que no es de confianza, incluso los recursos detrás de los firewalls de la red corporativa. El modelo de confianza cero funciona con el principio de "**no confiar en nadie y comprobarlo todo".**

La capacidad de los atacantes para eludir los controles de acceso convencionales está acabando con cualquier ilusión de que las estrategias de seguridad tradicionales son suficientes. Por lo tanto, al no confiar en la integridad de la red corporativa, se refuerza la seguridad.

En la práctica, esto significa que ya no asumimos que una contraseña es suficiente para validar a un usuario, sino que agregamos la autenticación multifactor para proporcionar comprobaciones adicionales. En lugar de conceder acceso a todos los dispositivos de la red corporativa, solo se permite el acceso de los usuarios a las aplicaciones o a los datos específicos que necesiten.

En este vídeo se muestra la metodología de confianza cero:

https://www.microsoft.com/es-mx/videoplayer/embed/RE4J3ms?postJsllMsg=true&autoCaptions=es-mx

Principios de GUID de confianza cero

El modelo de confianza cero tiene tres principios que guían y respaldan el modo de implementar la seguridad. Son los siguientes: la comprobación de forma explícita, el acceso con privilegios mínimos y asumir infracciones de seguridad.

- **Comprobación de forma explícita**. Autentique y autorice siempre el contenido en función de los puntos de datos disponibles, como la identidad del usuario, la ubicación, el dispositivo, el servicio o la carga de trabajo, la clasificación de los datos y las anomalías.
- **Acceso con privilegios mínimos**. Limite el acceso de los usuarios con acceso Just-in-Time y Just-Enough Access (JIT/JEA), LAS directivas de adaptación basadas en riesgos y LA protección de datos para proteger los datos y la productividad.
- **Asumir infracciones de seguridad**. Acceda al segmento mediante la red, el usuario, los dispositivos y la aplicación. Use el cifrado para proteger los datos y el análisis para obtener visibilidad, detectar amenazas y mejorar la seguridad.

Seis pilares básicos

En el modelo de confianza cero, todos los elementos funcionan juntos para proporcionar seguridad de un extremo a otro. Estos seis elementos son los pilares básicos del modelo de confianza cero:

- Las **identidades** pueden ser usuarios, servicios o dispositivos. Cuando una identidad intenta obtener acceso a un recurso, debe comprobarse mediante la autenticación sólida y seguir los principios de acceso con privilegios mínimos.
- Los **dispositivos** crean una superficie de ataque de gran tamaño a medida que los datos fluyen desde los dispositivos hasta las cargas de trabajo locales y en la nube. La supervisión del estado y el cumplimiento de los dispositivos es un aspecto importante de la seguridad.
- Las **aplicaciones** son la manera en que se consumen los datos. Esto incluye la detección de todas las aplicaciones que se usan, lo que a veces se denomina Shadow IT, ya que no todas las aplicaciones se administran de forma centralizada. Este pilar también incluye la administración de permisos y acceso.
- Los **datos** se deben clasificar, etiquetar y cifrar en función de sus atributos. En última instancia, los esfuerzos de seguridad están relacionados con la protección de los datos y garantizan que permanecen seguros cuando salen de los dispositivos, las aplicaciones, la infraestructura y las redes que controla la organización.
- La **infraestructura**, ya sea local o en la nube, representa un vector de amenazas. Para mejorar la seguridad, debe evaluar la versión, la configuración y el acceso JIT, y usar la telemetría para detectar ataques y anomalías. Esto le permite bloquear o marcar automáticamente el comportamiento de riesgo y tomar medidas de protección.
- Las **redes** deben segmentarse, incluida la microsegmentación en la red más profunda. Asimismo, es necesario emplear la protección contra amenazas en tiempo real, el cifrado, la supervisión y el análisis de un extremo a otro.

Una estrategia de seguridad que emplea los tres principios del modelo de Confianza cero en los seis pilares fundamentales ayuda a las empresas a ofrecer y aplicar la seguridad en toda su organización.

Descripción del cifrado y el código hash

Una manera de mitigar las amenazas de ciberseguridad más comunes es cifrar datos confidenciales o valiosos. El cifrado es el proceso para hacer que los datos aparezcan ilegibles e inútiles para visores no autorizados. Para usar o leer los datos cifrados, es necesario descifrarlos, lo que exige el uso de una clave secreta.

Hay dos tipos de cifrado de nivel superior: simétrico y asimétrico. El cifrado simétrico usa la misma clave para cifrar y descifrar los datos. El cifrado asimétrico usa un par de claves pública y privada. Cualquiera de las claves puede cifrar los datos, pero no se puede usar una sola clave para descifrar los datos cifrados. Para descifrarlos se necesita la otra clave emparejada. El cifrado asimétrico se usa para cosas como el acceso a sitios en Internet mediante el protocolo HTTPS y las soluciones de firma de datos electrónicas. El cifrado puede proteger los datos en reposo o en tránsito.

Cifrado de datos en reposo

Los datos en reposo son los datos que se almacenan en un dispositivo físico, como un servidor. Pueden estar almacenados en una base de datos o en una cuenta de almacenamiento, pero, independientemente de dónde estén almacenados, el cifrado de datos en reposo garantiza que los datos no se puedan leer sin las claves y los secretos necesarios para descifrarlos.

Si un atacante obtuviera una unidad de disco duro con datos cifrados, pero no tuviera acceso a las claves de cifrado, no podría leer los datos.

Cifrado de datos en tránsito

Los datos en tránsito son los que se están moviendo de una ubicación a otra, por ejemplo, por Internet o a través de una red privada. La transferencia segura se puede controlar mediante varias capas diferentes. Esto se puede hacer mediante el cifrado de los datos en el nivel de aplicación antes de enviarlos a través de una red. HTTPS es un ejemplo de cifrado en tránsito.

El cifrado de datos en tránsito protege los datos de observadores externos y proporciona un mecanismo para transmitirlos que limita el riesgo de exposición.

Cifrado de datos en uso

Un caso de uso común para el cifrado de datos en uso conlleva proteger los datos en un almacenamiento no persistente, como la RAM o la memoria caché de CPU. Esto se puede lograr

mediante tecnologías que crean un enclave (como si fuera una caja fuerte con llave) que protege los datos y los mantiene cifrados mientras la CPU los procesa.

Aplicación de algoritmo hash

El hash utiliza un algoritmo para convertir el texto en un valor hash de longitud fija *único* denominado hash. Cada vez que se aplica un algoritmo hash al mismo texto mediante el mismo algoritmo, se genera el mismo valor hash. Ese hash se puede usar como identificador único de los datos asociados.

El hash es diferente del cifrado, ya que no usa claves, y el valor al que se aplica el algoritmo hash no se descifra posteriormente en el original.

El hash se usa para almacenar contraseñas. Cuando un usuario escribe su contraseña, el mismo algoritmo que creó el hash almacenado crea un hash de la contraseña escrita. A continuación, se compara con la versión hash almacenada de la contraseña. Si coinciden, es que el usuario ha escrito correctamente la contraseña. Esto es más seguro que el almacenamiento de contraseñas de texto sin formato, pero los hackers también conocen los algoritmos hash. Dado que las funciones hash son deterministas (esto es, la misma entrada produce el mismo resultado), los hackers pueden usar los ataques de diccionario por fuerza bruta mediante el hash de las contraseñas. Por cada hash coincidente, obtienen la contraseña real. Para reducir este riesgo, a menudo las contraseñas se "cifran con sal". Esto hace referencia a que se agrega un valor aleatorio de longitud fija a la entrada de las funciones hash para crear valores hash únicos para la misma entrada.

Descripción de los conceptos de cumplimiento

Los datos son más importantes que nunca. Las organizaciones, las instituciones y sociedades enteras generan datos y dependen de ellos para que funcionar correctamente día a día. La gran escala de datos generados y la creciente dependencia de ellos significa que la privacidad y la protección de esos datos se han vuelto fundamentales. A medida que las organizaciones e instituciones mueven sus datos a las nubes del proveedor de servicios, con centros de datos de todo el mundo, entran en juego consideraciones adicionales.

Los organismos gubernamentales y los grupos del sector han aprobado reglamentos para ayudar a proteger y controlar el uso de los datos. Desde la información personal y financiera hasta la protección de datos y la privacidad, las organizaciones pueden tener la responsabilidad de cumplir decenas de reglamentos. A continuación se enumeran algunos conceptos y términos importantes relacionados con el cumplimiento de los datos.

- **Residencia de datos**: cuando se trata de cumplimiento, los reglamentos de residencia de datos rigen las ubicaciones físicas donde se pueden almacenar los datos y cómo y cuándo se pueden transferir, procesar o acceder a escala internacional. Estos reglamentos pueden variar significativamente en función de la jurisdicción.
- **Soberanía de datos**: otra consideración importante es la soberanía de los datos, el concepto de que los datos, especialmente los datos personales, están sujetos a las leyes y los reglamentos del país o la región donde se recopilan, conservan o procesan físicamente. Esto puede agregar una capa de complejidad cuando se trata de cumplimiento porque se puede recopilar el mismo fragmento de datos en una ubicación, almacenarse en otra y procesarse en otra, por lo que estaría sujeto a las leyes de diferentes regiones o países.
- **Privacidad de los datos**: proporcionar avisos y ser transparentes sobre la recopilación, el procesamiento, el uso y el uso compartido de los datos personales constituyen los principios fundamentales de las leyes y los reglamentos sobre privacidad. "Datos personales" hace referencia a cualquier información relativa a una persona física identificada o identificable. Las leyes sobre privacidad antes hacían referencia a "DCP" o "información de identificación personal", pero las leyes han ampliado la definición a cualquier dato que esté directamente vinculado o que se pueda vincular indirectamente a una persona. Las organizaciones están sujetas a una multitud de leyes, reglamentos, códigos de conducta, estándares específicos del sector y estándares de cumplimiento que rigen la privacidad de los datos y, por tanto, deben operar conforme a ellos.

En la mayoría de los casos, las leyes y los reglamentos no determinan ni prescriben las tecnologías específicas que las organizaciones deben usar para proteger los datos. Dejan a discreción de una organización identificar las tecnologías, las operaciones y otras medidas de protección de datos apropiadas que cumplan la normativa.