ONTI
Oficina Nacional de
Tecnologías de Información

Implementación de los principios de seguridad de la nube

Ver 1.0

REF: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

General

Para cada uno de los 14 principios, respondemos a tres preguntas:

1. ¿Cuál es el principio? Una descripción que le da al principio un cierto contexto
2. ¿Cuáles son los objetivos del principio? Aspectos clave para la aplicación a fin de lograr
3. ¿Cómo se aplica el principio? Tips para posibles implementaciones

Detalles y contexto de los 14 Principios de Seguridad en la Nube

1. Protección de datos en tránsito

Las redes de datos en tránsito de los usuarios deben protegerse adecuadamente contra la manipulación y la escucha clandestina.

2. Protección de activos y resiliencia

Los datos de los usuarios, y los activos que los almacenan o procesan, deben protegerse contra la manipulación física, la pérdida, el daño o la incautación.

3. Separación entre usuarios

Un usuario malicioso o comprometido del servicio no debe poder afectar el servicio o los datos de otro.

4. Marco de gobernanza

El proveedor de servicios debe tener un marco de gobernanza de la seguridad que coordine y dirija su gestión del servicio y de la información que contiene. Cualquier control técnico que se realice fuera de este marco se verá socavado de manera fundamental.

5. Seguridad operativa

El servicio debe ser operado y gestionado de forma segura para impedir, detectar o prevenir ataques. Una buena seguridad operativa no debería requerir procesos complejos, burocráticos, que requieran mucho tiempo o sean costosos.

6. Seguridad del personal

Cuando el personal del proveedor de servicios tiene acceso a sus datos y sistemas, necesita un alto grado de confianza en su fiabilidad. Una selección minuciosa, apoyada por una formación adecuada, reduce la probabilidad de que el personal de los proveedores de servicios se vea comprometido de forma accidental o maliciosa.

7. Desarrollo seguro

Los servicios deben diseñarse y desarrollarse para identificar y mitigar las amenazas a su seguridad. Los que no lo son pueden ser vulnerables a problemas de seguridad que podrían comprometer sus datos, causar pérdida de servicio o permitir otras actividades maliciosas.

8. Seguridad de la cadena de suministro

El prestador de servicios debe asegurarse de que su cadena de suministro respeta satisfactoriamente todos los principios de seguridad que el servicio pretende aplicar.

9. Gestión segura de usuarios

Su proveedor debe poner a su disposición las herramientas necesarias para que usted pueda gestionar de forma segura el uso de sus servicios. Las interfaces y procedimientos de gestión son una parte vital de la barrera de seguridad, evitando el acceso no autorizado y la alteración de sus recursos, aplicaciones y datos.

10. Identidad y autenticación

Todo acceso a las interfaces de servicio debe estar restringido a personas autenticadas y autorizadas.

11. Protección de la interfaz externa

Todas las interfaces externas o menos fiables del servicio deben ser identificadas y defendidas adecuadamente.

12. Administración de servicios seguros

Los sistemas utilizados para la administración de un servicio en la nube tendrán un acceso altamente privilegiado a ese servicio. Su compromiso tendría un impacto significativo, incluyendo los medios para eludir los controles de seguridad y robar o manipular grandes volúmenes de datos.

13. Información de auditoría para los usuarios

Se le deben proporcionar los registros de auditoría necesarios para supervisar el acceso a su servicio y los datos que contiene. El tipo de información de auditoría disponible para usted tendrá un impacto directo en su capacidad de detectar y responder a actividades inapropiadas o maliciosas dentro de plazos razonables.

14. Uso seguro del servicio

La seguridad de los servicios en la nube y de los datos que contienen puede verse socavada si se utiliza mal el servicio. En consecuencia, usted tendrá ciertas responsabilidades al utilizar el servicio para que sus datos estén adecuadamente protegidos.

1. Protección de datos en tránsito

Las redes de datos en tránsito de los usuarios deben protegerse adecuadamente contra la manipulación y la escucha clandestina.

Esto debería lograrse mediante una combinación de:

- **Protección de red** - negar a su atacante la capacidad de interceptar datos
- **Encriptación** - negar a su atacante la capacidad de leer los datos.

Aspectos Clave - Protección de datos en tránsito

Deberías considerar,

- Los datos en tránsito estén protegidos entre los dispositivos del usuario final y el servicio.
- Los datos en tránsito estén protegidos internamente dentro del servicio
- Los datos en tránsito estén protegidos entre el servicio y otros servicios (por ejemplo, cuando las API están expuestas).

Tips de Implementación - Protección de datos en tránsito

Puntos de ataque:

Para poner en peligro los datos en tránsito, un atacante necesitaría contar con acceso a la infraestructura por la que transitan los datos. Esto podría tomar la forma de acceso físico o acceso lógico si el atacante ha comprometido los componentes de software dentro del servicio.

Es más probable que los atacantes accedan a la infraestructura entre el usuario y el servicio, en lugar de a la infraestructura dentro del servicio. Sin embargo, el impacto de un atacante que accede a las comunicaciones internas del servicio probablemente sería significativamente mayor.

TLS.

Además de las protecciones de la capa de red a través de las redes internas o comunitarias, debería utilizar la protección TLS para los siguientes casos:

- Si se requiere confidencialidad adicional de los datos dentro de su organización o comunidad
- Para soportar la autenticación del usuario final y el control de acceso dentro de las aplicaciones

Ingresos y Egresos de usuarios

La incorporación y la baja de usuarios y cargas de trabajo pueden implicar la transferencia de datos masivos dentro o fuera del servicio. En este escenario, debería considerar la protección de datos durante el tránsito utilizando uno de los enfoques descritos anteriormente. Si se utilizan medios de almacenamiento para el tránsito de datos, éstos deben protegerse de acuerdo con el Principio 2: Protección de activos y resiliencia.

Aspecto	Descripción	Orientación
Servicio WAN privado	Usted accede al servicio a través de circuitos WAN privados ofrecidos por un proveedor de telecomunicaciones. La privacidad entre diferentes clientes de servicios WAN privados se debe generalmente a los protocolos de enrutamiento utilizados, como MPLS..	El uso de circuitos privados hará más difícil que un atacante tenga acceso a las comunicaciones. Estas conexiones normalmente no proporcionan protección criptográfica, pero es probable que sean difíciles de interceptar y procesar, lo que puede ser adecuado para sus necesidades. Las protecciones criptográficas, en caso de que decida desplegarlas, le proporcionarán una mayor confianza en la protección de la confidencialidad e integridad de sus comunicaciones.
SSL y TLS heredados	Se accede al servicio utilizando SSL o versiones heredadas de TLS (incluidas las versiones de TLS inferiores a 1.2).	No se recomienda el uso de versiones SSL o TLS anteriores a la versión 1.2. Existen vulnerabilidades conocidas en los protocolos que podrían ser manipuladas por un atacante para acceder a sus datos.

TLS (Versión 1.2 o superior)	Uso de TLS, configurado para utilizar suites de cifrado y tamaños de certificado recomendados.	La falta de garantía formal en las implementaciones de TLS significa que puede haber debilidades en la implementación. El uso de versiones recientes, compatibles y totalmente parcheadas de implementaciones de TLS procedentes de fuentes acreditadas ayudará a gestionar este riesgo.
Pasarela IPsec o TLS VPN	El servicio expone un TLS o Gateway IPsec VPN que se puede configurar para admitir un perfil criptográfico sólido.	
Conexiones de fibra óptica enlazadas	Las conexiones de fibra óptica enlazadas entre ubicaciones físicamente protegidas pueden utilizarse para proporcionar conexiones privadas entre centros de datos.	Se recomienda la validación independiente de la implementación de las conexiones de fibra óptica por parte del proveedor de servicios por parte de un experto reconocido.Tenga en cuenta que la seguridad de estos enlaces depende de una supervisión eficaz; ésta debería ser una de las consideraciones a tener en cuenta para cualquier validación independiente de la seguridad proporcionada.

2. Protección de activos y resiliencia

Los datos de los usuarios, y los activos que los almacenan o procesan, deben protegerse contra la manipulación física, la pérdida, el daño o la incautación.
Los aspectos a considerar son:

1. Ubicación física y jurisdicción legal
2. Seguridad del centro de datos
3. Protección de datos en reposo
4. Sanitización de los datos
5. Disposición final de equipos
6. Resiliencia física y disponibilidad

2.1 Ubicación física y jurisdicción legal

Para entender las circunstancias legales bajo las cuales se podría acceder a sus datos sin su consentimiento, debe identificar las ubicaciones en las que se almacenan, procesan y gestionan.

También tendrá que entender cómo se aplican los controles de tratamiento de datos dentro del servicio, en relación con la legislación vigente. La protección inadecuada de los datos de los usuarios puede dar lugar a sanciones legales y reglamentarias, o a daños a la reputación.

Aspectos Clave - Ubicación física y jurisdicción legal

Deberías considerar,

- En qué países se almacenarán, procesarán y gestionarán sus datos. También debe tener en cuenta la forma en que esto afecta al cumplimiento de la legislación pertinente, por ejemplo, la Ley de protección de datos (DPA).
- Si la(s) jurisdicción(es) legal(es) dentro de las cuales opera el proveedor de servicios son aceptables para usted

Tips de Implementación - Ubicación física y jurisdicción legal

Aspecto	Descripción	Orientación
Ubicaciones de procesamiento y almacenamiento desconocidas	El proveedor de servicios no ofrece información sobre la ubicación de los centros de datos para el almacenamiento y	En este escenario, usted no conoce las ubicaciones desde las que se puede acceder a sus datos, por lo que no será posible que

	procesamiento de la información y las cargas de trabajo.	usted comprenda plenamente la jurisdicción legal a la que están sujetos sus datos.
Lugares conocidos sólo para almacenamiento	El proveedor de servicios presenta información detallada sobre la ubicación de los centros de datos	El conocimiento de solo las ubicaciones de almacenamiento de sus datos es un riesgo potencial. Los datos también pueden estar disponibles en otras ubicaciones, como por ejemplo, donde se procesan o gestionan.
Lugares conocidos para el almacenamiento, el procesamiento y la gestión	El proveedor de servicios presenta información detallada sobre todas las ubicaciones en las que se almacenan y procesan los datos y dónde gestionan el servicio.	Este es el conjunto completo de ubicaciones físicas. Esto es necesario para poder comprender plenamente los riesgos relacionados con el acceso físico a sus datos. El nivel de confianza que tenga en las listas proporcionadas variará dependiendo de si depende de las afirmaciones del proveedor o si tiene una garantía adicional a través de una validación independiente. Otro factor importante es si el proveedor se compromete contractualmente a notificarle los cambios en la lista.

Notas adicionales - Ley de protección de datos

La legislación de protección de datos se aplicará si los datos personales se procesan en un servicio en la nube. La AAIP ha publicado Normativa sobre el cumplimiento de la Ley de Protección de Datos (LPDP) en relación con los servicios en la nube. La normativa tambien se refiere a las consideraciones para cuando los datos se transfieran a otros paises cuenten estos con legislacion adecuada o no. Ver Normativa AAIP sobre LPDP

Notas adicionales - Uso de sus datos

Usted debe considerar las implicaciones de cualquier derecho que el proveedor de servicios tendrá en relación con los datos almacenados dentro del servicio. Algunos acuerdos de uso permiten al proveedor de servicios emplear los datos de los usuarios para fines de marketing u otros fines. También debe comprobar si los acuerdos con el proveedor de servicios relativos al uso de sus datos son aceptables para usted y si no son contrarios a la legislación pertinente, como la LPDP. Ver Normativa AAIP sobre LPDP

2.2 Seguridad del centro de datos

Las ubicaciones utilizadas para proporcionar servicios cloud necesitan protección física contra el acceso no autorizado, la manipulación, el robo o la reconfiguración de los sistemas. Una protección inadecuada puede resultar en la divulgación, alteración o pérdida de datos.

Aspectos Clave Seguridad del centro de datos

Usted debe estar seguro de que las medidas de seguridad física empleadas por el proveedor son suficientes para su uso previsto del servicio.

Tips de Implementación - Seguridad del centro de datos

Aspecto	Descripción	Orientación
Desconocido	El proveedor de servicios no revela cómo están protegidos sus centros de datos.	En este escenario, usted estará tomando la palabra a los proveedores para que sus centros de datos estén debidamente protegidos. La decisión de hacerlo dependerá de la confianza intrínseca que usted tenga en el proveedor de servicios.
Controles conocidos	El proveedor del servicio divulga información sobre los controles de seguridad en torno a sus centros de datos (o los de sus proveedores).	Si el proveedor de servicios no menciona ninguna norma reconocida, Ud. deberá realizar su propia evaluación de los controles físicos que protegen estos centros de datos.

Cumple con una norma reconocida	El proveedor de servicios ha hecho certificar las protecciones de su centro de datos contra un estándar reconocido y apropiado que cubre la seguridad física. Los estándares apropiados incluyen: CSA CCM v3.X SSAE-16 / ISAE 3402	Las normas difieren en cuanto al nivel de detalle aplicado a los controles físicos. El alcance de la evaluación debe ser relevante para las ubicaciones en las que se puedan acceder a sus datos. Se puede obtener una validación independiente de que el alcance de una certificación es correcto para proporcionar seguridad en esta área.

2.3 Protección de datos en reposo

Para garantizar que los datos no estén disponibles para las partes no autorizadas con acceso físico a la infraestructura, los datos de los usuarios que se encuentren dentro del servicio deben protegerse independientemente del medio de almacenamiento en el que se encuentren. Si no se toman las medidas adecuadas, los datos pueden divulgarse inadvertidamente en medios desechados, perdidos o robados.

Aspectos Clave - Protección de datos en reposo

Debe tener la suficiente confianza de que los soportes de almacenamiento que contienen sus datos están protegidos contra el acceso no autorizado.

Tips de Implementación - Protección de datos en reposo

Los proveedores de servicios pueden utilizar cifrado, controles de seguridad física o una combinación de ambos para proteger los datos en reposo dentro del servicio.

Aspecto	Descripción	Orientación
Control de acceso físico	Una serie de normas son apropiadas para validar las protecciones de control de acceso físico. Estos están respaldados por una variedad de esquemas de certificación: CSA CCM v3.X SSAE-16 / ISAE 3402	Los niveles de control difieren entre las normas de seguridad física. El alcance de la evaluación debe ser relevante para aquellos lugares donde se pueda acceder a sus datos.
Inviabilidad de encontrar los datos de un cliente específico en un medio físico	El proveedor del servicio afirma que su escala, técnicas de ofuscación o fragmentación de datos hacen inviable que un determinado atacante con acceso físico a un centro de datos pueda localizar los datos de un cliente específico.	Es poco probable que haya una garantía independiente disponible para respaldar las afirmaciones del proveedor de servicios de que no es factible que alguien acceda a sus datos en un robo de un disco físico.
Cifrado de todos los medios físicos	El proveedor de servicios emplea el cifrado para garantizar que ningún dato se escriba en el disco de forma no cifrada.	La gestión de las claves utilizadas para cifrar los datos antes de que se almacenen es el mayor reto de este enfoque. Los errores en el uso de la criptografía o una gestión deficiente de las claves pueden dar lugar a la exposición de sus datos. También es importante entender si los productos de encriptación utilizados proporcionan la confianza que usted espera. Se recomiendan los productos que han sido evaluados según un buen estándar.

2.4 Sanitización de los datos

El proceso de aprovisionamiento, migración y desaprovisionamiento de recursos no debe dar lugar a un acceso no autorizado a los datos de los usuarios.

La sanitización inadecuada de los datos podría resultar en:

- Que sus datos sean conservados por el proveedor de servicios de forma indefinida
- Que sus datos sean accesibles a otros usuarios del servicio a medida que se reutilizan los recursos
- La pérdida o divulgación de sus datos en soportes desechados, perdidos o robados

Aspectos Clave - Sanitización de los datos

Deberías estar lo suficientemente seguro de que:

- Sus datos son borrados cuando los recursos son movidos o re-proveídos, cuando dejan el servicio o cuando usted solicita que sean borrados.
- Los soportes de almacenamiento que han conservado sus datos se desinfectan o se destruyen de forma segura al final de su vida útil.

Tips de Implementación - Sanitización de los datos

Aspecto	Descripción	Orientación
Ninguno/desconocido	El proveedor de servicios no puede explicar cómo se sanitiza el almacenamiento cuando es liberado por un usuario.	Puede ser que el enfoque del proveedor de servicios sobre su propia protección de datos en reposo (ver sección 2.3) le dé la confianza de que el almacenamiento reasignado no contendría datos de texto claro si se asignara a otro usuario. Si ese no es el caso, entonces usted podría optar por emplear el cifrado de los datos que almacena en el servicio.

Garantías de que los medios de comunicación no pueden ser abordados directamente	El proveedor de servicios puede ofrecer garantías de que los datos almacenados anteriormente no podrán ser tratados por otros después de su publicación.	Puede ser que el enfoque del proveedor de servicios sobre su propia protección de datos en reposo (ver sección 2.3) le dé la confianza de que el almacenamiento reasignado no contendría datos de texto claro si se asignara a otro usuario. Si ese es el caso, entonces sus garantías sobre cómo se reasignan los datos pueden proporcionarle toda la confianza que necesita. Sin embargo, dependiendo del servicio, también puede utilizar el cifrado para proteger adicionalmente sus datos almacenados.
Sobrescritura explícita del almacenamiento antes de la reasignación	El almacenamiento que ya no es necesario se sanitiza de acuerdo con una política específica antes de reasignarse a otro usuario.	Si sabe que los datos que ha utilizado anteriormente se sobrescriben antes de que se reasignen a otro usuario del servicio, esto le ayudará a estar seguro de que otro usuario no podrá acceder a sus datos. Al igual que con los otros métodos descritos anteriormente, puede ganar confianza adicional si el proveedor de servicios cifra todos los datos almacenados bajo claves específicas de usuario, o si cifra sus propios datos que almacena en el servicio.

2.5 Disposición final de equipos

Una vez que el equipo utilizado para prestar un servicio llega al final de su vida útil, debe ser eliminado de manera que no comprometa la seguridad del servicio ni los datos de los usuarios almacenados en el servicio.

Aspectos Clave - Disposición final de equipos

Deberías estar lo suficientemente seguro de que:

- Todo el equipo que potencialmente contenga sus datos, credenciales o información de configuración para el servicio sea identificado al final de su vida útil (o antes de ser reciclado).
- Todos los componentes que contengan datos sensibles sean sanitizados , eliminados o destruidos según corresponda.
- Las cuentas o credenciales específicas de los equipos redundantes sean revocadas para reducir su valor para un atacante.

Tips de implementación - Disposición final de equipos

Enfoque	Descripción	Orientación
Utilización de técnicas desconocidas o propietarias	-	En este caso, deberá confiar en el proveedor de servicios o llevar a cabo su propia evaluación de si los controles establecidos son apropiados.
Se sigue una norma reconocida para la eliminación de equipos	Una serie de normas incluyen controles que cubren la necesidad de una eliminación segura del equipo. Estos incluyen CSA CCM v3.X ISO/IEC 27001	Las normas a las que se hace referencia cubren la necesidad de una eliminación segura del equipo, en lugar de la validación del proceso. Vale la pena verificar el alcance de cualquier certificación para verificar que la existencia de controles apropiados fue cubierta como parte de la evaluación.

		Es probable que la validación independiente desempeñe un papel importante a la hora de proporcionar confianza en que los restos de sus datos no se pueden recuperar fácilmente de los equipos que se han desechado.
Se utiliza un servicio de destrucción de terceros	Se utiliza un servicio de destrucción especializado en la eliminación segura de equipos.	

2.6 Resiliencia física y disponibilidad

Los servicios tienen diferentes niveles de resiliencia, lo que afectará a su capacidad de funcionar normalmente en caso de fallos, incidentes o ataques. Un servicio sin garantías de disponibilidad puede dejar de estar disponible, potencialmente por períodos prolongados, independientemente del impacto en su negocio.

Aspectos Clave - Resiliencia física y disponibilidad

Debe tener la confianza suficiente de que los compromisos de disponibilidad del servicio, incluida su capacidad para recuperarse de las interrupciones, satisfacen las necesidades de su empresa.

Tips de implementación - Resiliencia física y disponibilidad

Enfoque	**Descripción**	**Orientación**
El proveedor de servicios se compromete a un Acuerdo de Nivel de Servicio (SLA)	Los compromisos contractuales o Acuerdos de Nivel de Servicio (SLAs) son utilizados por el proveedor de servicios para hacer compromisos sobre el nivel de disponibilidad del servicio.	Este enfoque puede proporcionar un mecanismo de compensación en caso de caidas o fallas del servicio, pero estas caidas o fallas no se evitarán si el diseño del servicio no es apropiado.

		Además, es beneficioso revisar los registros históricos del proveedor sobre la disponibilidad del servicio (véase el siguiente punto).
Revisión de datos históricos	El proveedor del servicio puede presentar evidencia histórica de la disponibilidad del servicio.	Usted debe evaluar esta evidencia y sacar sus propias conclusiones sobre si esto, junto con los compromisos y la reputación del proveedor de servicios, le dan suficiente confianza.
Análisis del diseño	El proveedor de servicios puede estar dispuesto a compartir información sobre cómo han diseñado su servicio para que sea resistente.	La revisión de esta información por parte de un experto en seguridad especializado proporcionaría una mayor confianza.

Notas adicionales - Resiliencia.

Debe evaluar si el proveedor de servicios puede cumplir con los requisitos de disponibilidad y resistencia que usted tiene. Se debe considerar que los servicios adquiridos con el apoyo de "mejores esfuerzos" no tienen apoyo garantizado.

3. Separación entre usuarios

Un usuario malicioso o comprometido del servicio no debe poder afectar el servicio o los datos de otro.
Los factores que afectan la separación de los usuarios incluyen:

- Donde se implementan los controles de separación - esto está fuertemente influenciado por el modelo de servicio (por ejemplo, IaaaS, PaaS, SaaS)
- Con quién está compartiendo el servicio - esto viene dictado por el modelo de implementación (por ejemplo, nube pública, privada o comunitaria).
- El nivel de garantía disponible en la aplicación de los controles de separación

Nota: En un servicio IaaaS debe considerar la separación proporcionada por los componentes de computación, almacenamiento y redes. Además, los servicios SaaS y PaaS construidos sobre IaaS pueden heredar algunas de las propiedades de separación de la infraestructura IaaS subyacente.

Para más información sobre la importancia de los requisitos de separación en los servicios cloud, consulte la seccion Separación y seguridad en la nube

Aspectos Clave - Separación entre usuarios

Debes...

- Comprender los tipos de usuarios con los que comparte el servicio o la plataforma
- Tener confianza en que el servicio proporciona una separación suficiente entre sus datos y el servicio y los de otros usuarios del servicio
- Tener confianza en que la gestión de su servicio se mantiene separada de otros usuarios (cubierto por separado como parte del Principio 9)

Tips de implementación - Separación de los usuarios

Tenga en cuenta que las combinaciones de los siguientes aspectos pueden ser complementarias. Cuando se utilizan en combinación, pueden proporcionar una mayor confianza en la fuerza de la separación dentro de un servicio.

Aspecto	Descripción	Orientación
Las tecnologías de virtualización (por ejemplo, un hipervisor) proporcionan separación entre los usuarios.	La separación del cómputo es proporcionada por un hipervisor. También se emplean técnicas de virtualización de redes y almacenamiento.	Suponiendo que se utilicen tecnologías de virtualización populares y bien diseñadas, es probable que esto proporcione una mayor separación que otros controles de software. Algunos productos de virtualización se han evaluado con arreglo a normas de seguridad bien definidas, como el plan de garantía de productos certificados.
Otros proveedores de software proporcionan separación entre los usuarios	Otros controles de software, como sistemas operativos, servidores web u otras aplicaciones, proporcionan separación entre los usuarios del servicio.	En este escenario, la superficie de ataque disponible para un usuario malintencionado es mucho mayor. Las vulnerabilidades o los problemas de mala configuración pueden provocar infracciones. En este escenario, debe tratar de ganar confianza en la implementación de los controles de separación. Busca evidencia de: .Pruebas periódicas de penetración de la infraestructura y de las aplicaciones web pertinentes .Revisiones de seguridad del diseño del servicio .Un enfoque de ingeniería que garantice la seguridad es una consideración clave en el desarrollo del servicio

Notas adicionales - Con quién está compartiendo el servicio

El grado de confianza que necesita establecer en las medidas de separación de usuarios empleadas en un servicio cloud dependerá de su uso previsto y del modelo de implementación del servicio.

- Para servicios de cloud **privada**.

Debido a que se trata de una sola organización debe tener una buena comprensión de todos sus usos para el entorno de la nube, es posible que se sienta cómodo con sólo tener una garantía bastante limitada en la separación del servicio.

- Para servicios **comunitarios** en la nube.

Cuando usted confía en la comunidad y se sabe que sus miembros practican un buen nivel de higiene (tal vez incluso se rigen por un código de conducta), la evidencia de que se realizan regularmente pruebas de penetración de buen alcance puede darle suficiente confianza en la separación proporcionada.

- Para servicios **públicos** en la nube.

Usted debe considerar la fortaleza de la separación requerida, dado que otros consumidores del servicio pueden ser activamente hostiles hacia usted. Si se necesita un mayor nivel de confianza, además de las pruebas de penetración, puede ser conveniente obtener garantías en el diseño del servicio y las prácticas de ingeniería del proveedor de servicios.

Notas adicionales - Test de penetración

Un test de penetración bien definido (y la implementación de sus recomendaciones) puede dar confianza en que los productos y los controles de seguridad probados se han configurado de acuerdo con las buenas prácticas y en que no existen vulnerabilidades comunes o conocidas públicamente en los componentes probados, en el *momento del test*.

Un test de penetración normalmente no evalúa los productos o componentes en busca de vulnerabilidades desconocidas hasta ahora.

Asegúrese de que sus probadores de penetración estén debidamente cualificados. Por ejemplo, personas certificadas bajo los esquemas CHECK, CREST o Tiger.

La revisión independiente del alcance de una prueba de penetración, y la revisión de las mitigaciones que identificó, dará un mayor grado de confianza en que las pruebas de penetración lograron con éxito los objetivos establecidos anteriormente.

4. Marco de gobernanza

El proveedor de servicios debe tener un marco de gobernanza de la seguridad que coordine y dirija su gestión del servicio y de la información que contiene. Cualquier control técnico que se realice fuera de este marco se verá socavado de manera fundamental.

Contar con un marco de gobernanza eficaz garantizará que los procedimientos, el personal y los controles físicos y técnicos sigan funcionando durante toda la vida útil de un servicio. También debe responder a los cambios en el servicio, a los avances tecnológicos y a la aparición de nuevas amenazas.

Aspectos Clave -Marco de gobernanza

Usted debe tener la suficiente confianza de que el servicio tiene un marco de gobernanza y procesos que son apropiados para el uso al que se destina.

Por lo general, la buena gobernanza proporciona:

- Un representante de la organización claramente identificado y nombrado (o una persona con la autoridad delegada directa) que sea responsable de la seguridad del servicio cloud. Normalmente se trata de alguien con el título de"Director de Seguridad","Director de Información" o"Director Técnico".
- Un marco documentado para la gobernanza de la seguridad, con políticas que rigen los aspectos clave de la seguridad de la información relevantes para el servicio.
- La seguridad y la seguridad de la información que forman parte de los mecanismos de información sobre riesgos financieros y operativos del proveedor de servicios, lo que garantiza que los responsables de la organización se mantenga informada de los riesgos de seguridad e información.
- Procesos para identificar y asegurar el cumplimiento de los requisitos legales y reglamentarios aplicables.

Tips de implementación - Marco de gobernanza

Aspecto	Descripción	Orientación
Afirmación de que se cumplen las metas	El proveedor del servicio afirma que los 4 puntos anteriores son cumplidos por el proveedor en relación con el servicio.	Al igual que con todas las afirmaciones de los proveedores de servicios, usted tendría que decidir si está satisfecho con el nivel

		de confianza que esto le proporciona.
Conformidad con una norma reconocida	Algunas normas de seguridad comunes incluyen controles que cubren hasta qué punto un marco de gobernanza gestiona un servicio en particular. Los ejemplos incluyen CSA CCM v3.X ISO/IEC 27001	Las normas difieren en el nivel de detalle aplicado. El alcance de cualquier certificación de apoyo debe ser validado para asegurar que se cubran los objetivos del marco de gobernanza establecidos anteriormente.

5. Seguridad operativa

El servicio debe ser operado y gestionado de forma segura para impedir, detectar o prevenir ataques. Una buena seguridad operativa no debería requerir procesos complejos, burocráticos, que requieran mucho tiempo o sean costosos.
Hay cuatro elementos a considerar:

1. Gestión de la configuración y de los cambios - debe asegurarse de que los cambios en el sistema han sido debidamente probados y autorizados. Los cambios no deben alterar inesperadamente las propiedades de seguridad
2. Gestión de vulnerabilidades: debe identificar y mitigar los problemas de seguridad en los componentes de los componentes.
3. Vigilancia de protección: debe implementar medidas para detectar ataques y actividades no autorizadas en el servicio.
4. Gestión de incidentes: asegúrese de que puede responder a los incidentes y recuperar un servicio seguro y disponible.

5.1 Configuración y gestión de cambios

Debe tener una idea precisa de los activos que componen el servicio, junto con sus configuraciones y dependencias.

Deben identificarse y gestionarse los cambios que puedan afectar a la seguridad del servicio. Se deben detectar los cambios no autorizados.

Cuando el cambio no se gestiona de forma eficaz, las vulnerabilidades de seguridad pueden introducirse involuntariamente en un servicio e incluso cuando existe conciencia de la vulnerabilidad, es posible que no se pueda mitigar por completo.

Aspectos Clave -Configuración y gestión de cambios

Deberías tener confianza en:

- El estado, la ubicación y la configuración de los componentes de servicio (tanto de hardware como de software) se controlan a lo largo de su vida útil.
- Los cambios en el servicio se evalúan en función del impacto potencial en la seguridad. Debe gestionarse y realizar un seguimiento hasta su finalización.

Tips de Implementación - Configuración y gestión de cambios

Aspecto	Descripción	Orientación
Afirmación de que se cumplen las metas	El proveedor de servicios afirma que se han alcanzado los objetivos anteriores.	Al igual que con todas las afirmaciones de los proveedores de servicios, debe decidir si está satisfecho con el nivel de confianza que esto le proporciona.
Conformidad con una norma reconocida	Una serie de normas incluyen controles que cubren la necesidad de procesos de configuración y gestión de cambios: CSA CCM v3.X ISO/IEC 27001	Los buenos procesos de gestión de cambios y configuración reducen (pero no eliminan) la posibilidad de que se introduzcan vulnerabilidades en la configuración de un servicio. Los estándares difieren en cuanto al nivel de detalle aplicado, y los referenciados cubren la necesidad de gestión de la configuración y el cambio, en lugar de la validación del proceso. Vale la pena comprobar el alcance de cualquier certificación para verificar que los procesos de configuración y de gestión de cambios fueron cubiertos como parte de la evaluación. Sin una buena gobernanza del servicio (véase el Principio 4), es probable que las prácticas de gestión del cambio y la configuración sean ineficaces.

Notas adicionales - Priorización de los cambios

Es importante contar con procesos efectivos de gestión del cambio. Pero también debe darse cuenta de que hasta que el proceso esté completo, su servicio seguirá siendo vulnerable. En consecuencia, los cambios deben ser priorizados de acuerdo a la severidad del riesgo.

5.2 Gestión de vulnerabilidades

Los proveedores de servicios deben contar con procesos de gestión para identificar, clasificar y mitigar las vulnerabilidades. Los servicios que no lo hacen, se volverán rápidamente vulnerables a los ataques utilizando métodos y herramientas conocidos públicamente.

Aspectos Clave - Gestión de vulnerabilidades

Deberías tener confianza en que,

- Se evalúan las nuevas amenazas, vulnerabilidades o técnicas de explotación potenciales que podrían afectar a su servicio y se toman medidas correctivas.
- El proveedor del servicio supervisa las fuentes de información pertinentes relacionadas con las técnicas de amenaza, vulnerabilidad y explotación.
- La gravedad de las amenazas y vulnerabilidades se considera dentro del contexto del servicio y esta información se utiliza para priorizar la implementación de mitigaciones.
- Utilizando un proceso de gestión de cambios adecuado, se hace un seguimiento de las vulnerabilidades conocidas hasta que se hayan implementado las medidas de mitigación.
- Usted conoce las escalas de tiempo de los proveedores de servicios para implementar las mitigaciones y está satisfecho con ellas.

Tips de Implementación - Gestión de vulnerabilidades

Aspecto	Descripción	Orientación
Afirmación de que se cumplen las metas	El proveedor de servicios afirma que se han alcanzado los objetivos anteriores.	Al igual que con todas las afirmaciones de los proveedores de servicios, debe decidir si está satisfecho con el nivel de confianza que esto le proporciona.

Conformidad con una norma reconocida	Una serie de estándares son apropiados para soportar la gestión de vulnerabilidades. Estos tienen sus propios mecanismos de certificación: ISO/IEC 30111:2013 CSA CCM v3.X ISO/IEC 27001	Ningún proceso de gestión de vulnerabilidades puede defenderse contra vulnerabilidades desconocidas ("día cero"). Ninguno de los estándares referenciados establece explícitamente plazos aceptables para la mitigación, por lo que vale la pena considerar sus requerimientos. Como mínimo, le aconsejamos que busque servicios que soporten la aplicación de parches o la gestión de vulnerabilidades dentro de los plazos que se indican a continuación.

Notas adicionales - Plazos de mitigación

Los exploits para vulnerabilidades conocidas están frecuentemente disponibles, a través de Internet, a las pocas horas de su publicación. *Las organizaciones que mitigan y parchean vulnerabilidades en sus servicios rápidamente tienen ventanas de vulnerabilidad más pequeñas.*

Debe saber si su proveedor de servicios repara las vulnerabilidades dentro de plazos aceptables.

Si hay pruebas que sugieren que una vulnerabilidad está siendo explotada activamente en el campo, los proveedores de servicios tendrán que poner en marcha medidas de mitigación de **inmediato**.

Si no hay pruebas de que se esté explotando activamente una vulnerabilidad, las siguientes escalas de tiempo deberían considerarse buenas prácticas mínimas:

- Los parches'críticos' deben desplegarse en cuestión de horas.
- Los parches'importantes' deben desplegarse en un plazo de 2 semanas a partir de la disponibilidad de un parche.

- Otros" parches desplegados dentro de las 8 semanas siguientes a la disponibilidad de un parche.

Crítico', `Importante' y `Otro' están alineados con los siguientes sistemas comunes de puntuación de vulnerabilidades:

- Clasificación de la gravedad de la vulnerabilidad: 'Alta', 'Media' y 'Baja' respectivamente (éstas, a su vez, están alineadas con las puntuaciones del CVSS establecidas por el NIST).
- Clasificaciones del Sistema de Clasificación de Severidad del Boletín de Seguridad de Microsoft: 'Crítico', 'Importante' y los dos niveles restantes ('Moderado' y 'Bajo') respectivamente.

5.3 Vigilancia de la protección

Es poco probable que un servicio que no supervise eficazmente los ataques, el uso indebido y el mal funcionamiento detecte ataques (tanto exitosos como no exitosos). Como resultado, será incapaz de responder rápidamente a los compromisos potenciales de sus entornos y datos.

Aspectos Clave -Vigilancia de la protección

Deberías tener confianza en que,

- El servicio genera eventos de auditoría adecuados para apoyar la identificación efectiva de actividades sospechosas.
- Estos eventos se analizan para identificar posibles compromisos o uso inapropiado de su servicio.
- El proveedor del servicio toma las medidas oportunas y oportunas para hacer frente a los incidentes.

Tips de Implementación - Monitoreo de protección

Aspecto	Descripción	Orientación
Afirmación de que se cumplen las metas	El proveedor de servicios afirma que se han alcanzado los objetivos anteriores.	Al igual que con todas las afirmaciones de los proveedores de servicios, debe decidir si está satisfecho con el nivel de confianza que esto le proporciona.

Conformidad con una norma reconocida	Una serie de normas incluyen controles que cubren la necesidad de procesos eficaces de supervisión de la protección: CSA CCM v3.X ISO/IEC 27001	Las normas difieren en cuanto al nivel de detalle aplicado, y las referidas cubren la necesidad de un seguimiento eficaz de la protección, en lugar de la validación de los controles establecidos. Vale la pena revisar el alcance de cualquier certificación para verificar que los controles de monitoreo de protección fueron cubiertos como parte de la evaluación. También es aconsejable verificar que la certificación haya sido realizada por una parte independiente y experta.

Notas adicionales - Seguimiento y análisis

Es poco probable que los servicios que no recopilan información relevante de contabilidad y auditoría detecten y respondan rápidamente a los ataques o intentos de ataques.

Y cuando los ataques se detectan a través de otros mecanismos, será difícil determinar el alcance, la duración y la gravedad de la amenaza si no se dispone de datos de auditoría pertinentes.

Es igualmente improbable que los servicios que recopilan información contable y de auditoría*, pero que no disponen de un análisis eficaz* de dicha información, *detecten y respondan rápidamente a los ataques*. No hay manera de saber si los datos no examinados serán suficientes para apoyar una investigación o enjuiciamiento, en caso de que ocurra.

Notas adicionales - Responsabilidad de supervisión

En los servicios IaaS y PaaS los usuarios ejecutan sus aplicaciones o software sobre el servicio. Es *poco probable que* los proveedores ofrezcan supervisión de protección para estas aplicaciones, *a menos que* el consumidor y el proveedor de servicios hayan trabajado juntos para diseñar una solución adecuada.Ver el concepto de Responsabilidad Compartida en la Gestión de la Seguridad en infraestructura

En estos escenarios, es típicamente usted, el usuario del servicio, quien será responsable (y a menudo el mejor situado) de identificar los ataques contra sus aplicaciones o software. Para ello necesitará sus propios sistemas de monitorización.

5.4 Gestión de incidentes

A menos que existan procesos de gestión de incidentes cuidadosamente planificados, es probable que se tomen malas decisiones cuando se produzcan incidentes, lo que podría exacerbar el impacto general en los usuarios.

Estos procesos no tienen por qué ser complejos ni requerir grandes cantidades de descripción, pero una buena gestión de incidencias minimizará el impacto en los usuarios de los problemas de seguridad, fiabilidad y medio ambiente de un servicio.

Aspectos Clave - Gestión de incidentes

Deberías tener confianza en que,

- Se han establecido procesos de gestión de incidentes para el servicio y se despliegan activamente en respuesta a los incidentes de seguridad.
- Existen procesos predefinidos para responder a tipos comunes de incidentes y ataques.
- Existe un proceso y una ruta de contacto definidos para la notificación de incidentes de seguridad por parte de consumidores y entidades externas.
- Los incidentes de seguridad que sean relevantes para usted se notificarán en plazos y formatos aceptables.

Tips de Implementación - Gestión de incidencias

Aspecto	Descripción	Orientación
Afirmación de que se cumplen las metas	El proveedor de servicios afirma que se han cumplido los objetivos anteriores.	Al igual que con todas las afirmaciones de los proveedores de servicios, debe decidir si está satisfecho con el nivel de confianza que esto le proporciona.
Conformidad con una norma reconocida	Una serie de normas incluyen la necesidad de una gestión de incidentes en línea con los objetivos establecidos. Éstos	Las normas a las que se hace referencia difieren en cuanto al nivel de detalle aplicado. Algunos cubren los

	cuentan con sus propios procesos de certificación de apoyo: ISO/IEC 27035-1:2016 CSA CCM v3.X ISO/IEC 27001	controles de gestión de incidentes en detalle, mientras que otros simplemente requieren que exista un proceso de gestión de incidentes. Vale la pena comprobar el alcance de cualquier certificación para verificar lo que realmente se evaluó. También es aconsejable verificar que la certificación haya sido realizada por una parte independiente y experta.

Notas adicionales - Ataques significativos y alta disponibilidad

Toda persona que publique servicios que puedan ser objeto de ataques significativos (en términos de volumen o capacidad técnica) debe recurrir a proveedores que puedan demostrar unos procedimientos de gestión de incidentes sólidos, bien probados y ensayados.

Los ataques de denegación de servicio contra infraestructuras públicas por parte de hakers o delincuentes graves con fines lucrativos pueden ser una prueba particularmente exigente de los procesos de respuesta a incidentes, especialmente para los usuarios con un requisito de alta disponibilidad.

6. Seguridad del personal

Cuando el personal del proveedor de servicios tiene acceso a sus datos y sistemas, necesita un alto grado de confianza en su fiabilidad. Una selección minuciosa, apoyada por una formación adecuada, reduce la probabilidad de que el personal de los proveedores de servicios se vea comprometido de forma accidental o maliciosa.

El proveedor del servicio debe someter al personal a controles de seguridad y a una formación periódica en materia de seguridad. El personal que desempeña estas funciones debe comprender sus responsabilidades. Los proveedores deben dejar en claro cómo seleccionan y administran al personal dentro de los roles privilegiados.

Aspectos Clave - Seguridad del personal

Deberías estar seguro de que:

- El nivel de control de seguridad realizado al personal del proveedor de servicios con acceso a su información, o con capacidad para afectar su servicio, es apropiado
- El número mínimo de personas necesarias tienen acceso a su información o podrían afectar a su servicio

Tips de Implementación - Seguridad del personal

Aspecto	Descripción	Orientación
No se ha realizado el “escaneado” de personal	Algunas organizaciones pueden no estar dispuestas o ser incapaces de realizar controles de selección de personal.	Las personas no examinadas pueden tener la capacidad de acceder a su información o afectar su servicio.
Control de personal realizado pero no conforme a la norma BS7858:2012 (o similar)	La norma BS7858:2012 (o similar)establece un estándar básico para la selección de personal. Muchas compañías multinacionales realizarán verificaciones de antecedentes del personal que cumplan con los requisitos de esta norma, aunque en algunos países	En estos casos, le recomendamos que solicite al proveedor de servicios que describa las funciones de control de seguridad del personal que lleva a cabo en el personal con acceso a sus datos, o la capacidad de afectar a los servicios de los usuarios. Tendrá

	no es posible realizar todas las verificaciones.	que juzgar si eso es suficiente. Cuando los proveedores de servicios no pueden verificar la identidad, comprobar si hay condenas penales no cumplidas y el derecho al trabajo del personal, existe un mayor riesgo de amenazas internas.
Selección de personal realizada conforme a la norma BS7858:2012 (o similar)	Se ha establecido un sistema de selección de personal que incluye o supera los requisitos de la norma BS7858:2012 (o similar)	Aunque la selección de personal es valiosa, vale la pena señalar que es extremadamente difícil diseñar sistemas capaces de defender los datos de los ataques de un usuario privilegiado que es a la vez hábil y motivado. Es probable que el personal del proveedor de servicios con funciones privilegiadas pueda acceder a sus datos y/o afectar la fiabilidad de su servicio. Si es posible, puede que le resulte útil comprender el enfoque del proveedor de servicios para detectar a los posibles miembros malintencionados y utilizar esta información como parte de su decisión de gestión de riesgos.

Información adicional - Autenticación y protección de la administración de servicios

Cualquiera que trabaje para el proveedor de servicios que tenga acceso a sus datos, o que tenga la capacidad de afectar a su servicio, debe estar fuertemente autenticado. También necesitan administrar su uso del servicio de una manera segura. Vale la pena considerar a

estos usuarios como un caso especial cuando revise el Principio 10 - Identidad y autenticación, y si administrarán el servicio de forma segura como parte del Principio 12 - Administración de servicios seguros.

7. Desarrollo seguro

Los servicios deben diseñarse y desarrollarse para identificar y mitigar las amenazas a su seguridad. Los que no lo son pueden ser vulnerables a problemas de seguridad que podrían comprometer sus datos, causar pérdida de servicio o permitir otras actividades maliciosas.

Aspectos Clave - Desarrollo seguro

Deberías estar seguro de que:

- Se examinan las amenazas nuevas y cambiantes y se mejora el servicio en consonancia con ellas.
- El desarrollo se lleva a cabo de acuerdo con las buenas prácticas de la industria en lo que respecta al diseño, la codificación, las pruebas y el despliegue seguros.
- Existen procesos de gestión de la configuración para garantizar la integridad de la solución mediante el desarrollo, las pruebas y la implementación.

Tips de Implementación - Desarrollo seguro

Aspecto	Descripción	Orientación
Los enfoques de ingeniería consideran la seguridad como un factor importante	El proveedor de servicios afirma que implementa una serie de controles para garantizar la seguridad de su servicio.	En este caso, deberá llevar a cabo su propia evaluación para determinar si los controles establecidos son adecuados.
El enfoque de ingeniería se adhiere a un estándar de desarrollo seguro o a una buena práctica reconocida.	Existe una serie de normas de seguridad o guías de buenas prácticas que los proveedores de servicios pueden alegar que apoyan el logro de los objetivos antes mencionados. Estos incluyen ISO/IEC 27034 Ver también el punto #5 del Codigo de Buenas Prácticas para el desarrollo de Software	Es tranquilizador que el proveedor de servicios afirme que implementa uno de estos estándares, pero sin una confirmación independiente de que usted necesitará juzgar si eso le da suficiente confianza en que todas las partes del sistema están diseñadas de manera segura.

	Público : 5. Protegé al software y a los usuario	
Revisión independiente del enfoque de ingeniería con respecto a un estándar de desarrollo seguro reconocido	Existen una serie de normas de seguridad con mecanismos de certificación de apoyo que podrían utilizarse para demostrar la conformidad con los objetivos antes mencionados. Estos incluyen ISO/IEC 27034 CSA CCM v3.X ISO/IEC 27001	Es aconsejable comprobar que la certificación ha sido realizada por una parte debidamente independiente y reconocida y que el alcance de la evaluación incluye los aspectos de gestión de incidentes requeridos.

Notas adicionales - Requisitos de desarrollo seguro

Un desarrollo seguro no significa que todo el desarrollo deba realizarse en la propia empresa, en instalaciones seguras o por personal altamente cualificado. Si bien estos enfoques pueden ser apropiados para componentes especializados, a menudo será mejor elegir componentes maduros, soportados de forma independiente y listos para su uso.

La seguridad debe ser considerada a lo largo del diseño y desarrollo del servicio. Por ejemplo, durante el desarrollo de nuevas características, los ataques potenciales deben ser evaluados y se deben diseñar mitigaciones efectivas para enfrentarlos. Se debe tener cuidado para equilibrar la seguridad, el costo y la facilidad de uso.

Los proveedores de servicios deben asegurarse, cuando adquieren servicios, componentes de software o servicios de desarrollo a terceros, de que las prácticas de desarrollo del proveedor son convenientemente seguras. Esto debería lograrse mediante un proceso establecido de la cadena de suministro (véase Principio 8 . Seguridad en la Cadena de Suministro).

8. Seguridad de la cadena de suministro

El prestador de servicios debe asegurarse de que su cadena de suministro respeta satisfactoriamente todos los principios de seguridad que el servicio pretende aplicar.

Los servicios cloud suelen depender de productos y servicios de terceros. Por consiguiente, si no se aplica este principio, el compromiso de la cadena de suministro puede afectar la seguridad del servicio y afectar a la aplicación de otros principios de seguridad.

Aspectos Clave - Seguridad de la cadena de suministro

Usted entiende y acepta:

- Cómo se comparte su información con, o se hace accesible a, terceros proveedores y *sus* cadenas de suministro.
- Cómo los procesos de adquisición del proveedor de servicios imponen requisitos de seguridad a terceros proveedores.
- Cómo gestiona el proveedor de servicios los riesgos de seguridad de terceros proveedores.
- Cómo gestiona el proveedor de servicios la conformidad de sus proveedores con los requisitos de seguridad.
- Cómo verifica el proveedor de servicios que el hardware y software utilizado en el servicio es auténtico y no ha sido manipulado.

Tips de Implementación - Seguridad de la cadena de suministro

Aspecto	Descripción	Orientación
Compromisos	El proveedor de servicios le asegura que los controles de seguridad que son importantes para usted son transitados a través de su cadena de suministro.	En este caso, deberá llevar a cabo su propia evaluación para determinar si los controles establecidos son adecuados.
Evaluado mediante la aplicación de normas apropiadas	Los controles de seguridad se aplican en la cadena de suministro mediante la aplicación de una norma pertinente.	Es aconsejable comprobar que la certificación ha sido realizada por una parte debidamente independiente y reconocida y que el alcance de la evaluación incluye los aspectos de la

	Existen varias normas de seguridad con mecanismos de certificación de apoyo. Estos incluyen ISO/IEC 27001 ISO/PAS 28000:2007	cadena de suministro requeridos.

Notas adicionales - Servicios por niveles

Los servicios cloud suelen construirse sobre productos IaaaS o PaaS de terceros. Esta es una valiosa oportunidad para reutilizar componentes de confianza, pero es importante identificar qué parte es responsable de implementar qué funciones de seguridad.

Estos servicios por niveles pueden resultar en una situación más compleja cuando se trata de entender la Separación y seguridad en la nube. Por ejemplo, una comunidad SaaS puede separar diferentes usuarios con controles de software de aplicación. Sin embargo, puede haber sido construido sobre una oferta de IaaaS de nube pública, donde los controles de separación se implementan en el hipervisor. Por lo tanto, los controles reales pueden ser diferentes en la práctica de lo que aparecen por primera vez.

Si su aplicación o datos son particularmente sensibles, necesitará considerar toda la pila de servicios subyacente como parte de cualquier evaluación de seguridad. Será difícil ganar un alto grado de confianza en la seguridad de cualquier servicio construido sobre bases que usted no entiende.

9. Gestión segura de usuarios

Su proveedor debe poner a su disposición las herramientas necesarias para que usted pueda gestionar de forma segura el uso de sus servicios. Las interfaces y procedimientos de gestión son una parte vital de la barrera de seguridad, evitando el acceso no autorizado y la alteración de sus recursos, aplicaciones y datos.

Los aspectos a considerar son:

- Autenticación de usuarios a interfaces de gestión y canales de soporte
- Separación y control de acceso dentro de las interfaces de gestión

9.1 Autenticación de usuarios a interfaces de gestión y canales de soporte

Para mantener un servicio seguro, los usuarios deben estar debidamente autenticados antes de que se les permita realizar actividades de gestión, informar de fallos o solicitar cambios en el servicio.

Estas actividades pueden realizarse a través de un portal web de gestión de servicios, o a través de otros canales, como el teléfono o el correo electrónico. Es probable que incluyan funciones tales como la provisión de nuevos elementos de servicio, la gestión de cuentas de usuario y la gestión de datos de consumidores.

Los proveedores de servicios deben asegurarse de que todas las solicitudes de gestión que puedan tener un impacto en la seguridad se realicen a través de canales seguros y autenticados. Si los usuarios no están fuertemente autenticados, entonces un impostor puede ser capaz de realizar con éxito acciones privilegiadas, socavando la seguridad del servicio o de los datos.

Aspectos Clave -Autenticación de usuarios a interfaces de gestión y canales de soporte

Deberías tener suficiente confianza en,

- Conocer todos los mecanismos por los que el proveedor de servicios aceptaría sus solicitudes de gestión o de asistencia (teléfono, portal web, correo electrónico, etc.).
- Que sólo las personas autorizadas de su organización pueden utilizar estos mecanismos para influir en su uso del servicio (el Principio 10 Identidad y Autenticación puede ayudarle a considerar la fuerza de la identificación y autenticación de los usuarios en cada uno de estos mecanismos).

Tips de Implementación - Autenticación a la gestión Interfaces y soporte

Aspecto	Descripción	Orientación
Autenticación sólida en el lugar	El proveedor de servicios afirma que dispone de controles suficientes para garantizar que sólo los usuarios autorizados de su organización puedan afectar a su cuenta a través de los canales de soporte.	Vale la pena preguntar a su proveedor de servicios cómo comprueban que sólo los usuarios autorizados pueden afectar a su cuenta. Es posible que desee llevar a cabo sus propias pruebas para confirmar que está satisfecho con las medidas de seguridad establecidas.
Autenticación fuerte en el lugar, que está sujeta a un ejercicio regular.	Como en el caso anterior, pero el proveedor de servicios puede demostrar que comprueba regularmente su seguridad a través de estos canales (por ejemplo, mediante el uso de técnicas de ingeniería social).	Si bien el ejercicio de la fuerza de la autenticación es una buena manera de ganar confianza, debe tener en cuenta que sólo prueba los mecanismos de autenticación en un momento dado, por lo que es importante que las pruebas se realicen con frecuencia. Desafortunadamente, no existen normas reconocidas para evaluar la calidad de las pruebas de ingeniería social. Es mejor asegurarse de que se utilicen probadores experimentados y de buena reputación.

9.2 Separación y control de acceso dentro de las interfaces de gestión

Muchos servicios en la nube se gestionan a través de aplicaciones web o API. Estas interfaces son una parte clave de la seguridad del servicio. Si los usuarios no están adecuadamente separados dentro de las interfaces de gestión, un usuario puede afectar al servicio o modificar los datos de otro.

Sus cuentas administrativas privilegiadas probablemente tengan acceso a grandes volúmenes de datos. Limitar los permisos de los usuarios individuales a los absolutamente necesarios puede ayudar a limitar los daños causados por usuarios malintencionados, credenciales comprometidas o dispositivos comprometidos.

El control de acceso basado en funciones proporciona un mecanismo para lograrlo y es probable que sea una capacidad particularmente importante para los usuarios que gestionan despliegues de mayor envergadura.

La exposición de las interfaces de gestión a redes menos accesibles (por ejemplo, redes comunitarias en lugar de redes públicas) dificulta que los atacantes lleguen a ellas y las ataquen, ya que primero tendrían que acceder a una de estas redes. En el Principio 11 Protección de la Interfaz externa se ofrece orientación sobre la evaluación de los riesgos de exponer las interfaces a diferentes tipos de redes.

Aspectos Clave -Separación y control de acceso dentro de las interfaces de gestión

Deberías,

- Tener confianza en que otros usuarios no pueden acceder, modificar o afectar de otro modo a la gestión de su servicio
- Gestionar los riesgos del acceso privilegiado utilizando un sistema como el "principio del menor privilegio".
- Comprender cómo se protegen las interfaces de gestión (véase el Principio 11 Protección de la Interfaz externa) y qué funcionalidad exponen

Tips de Implementación - control de acceso dentro de las interfaces de gestión

Aspecto	Descripción	Orientación
Sin interfaz de gestión de servicios digitales para que los usuarios administren su servicio	Algunos servicios pueden no tener una interfaz digital para que los usuarios administren su uso del servicio. Esto puede deberse a que el servicio es muy sencillo o no tiene aspectos que los usuarios puedan gestionar.	-
Control de acceso implementado en el software	La separación entre los usuarios de las interfaces de	Las interfaces de gestión de servicios suelen ser altamente privilegiadas, por

	gestión de servicios digitales se realiza en el software	lo que es importante que tenga la seguridad de que están bien diseñadas y mantenidas.
Control de acceso implementado en el software, sujeto a pruebas periódicas	Como en el caso anterior, pero se utilizan pruebas periódicas, incluidas pruebas de penetración, para evaluar la fuerza de la separación dentro de las interfaces de gestión de servicios digitales.	Las pruebas de penetración deben tener un buen alcance para garantizar que proporcionan confianza en la seguridad de las interfaces de gestión de servicios. Cabe señalar que una prueba de penetración normalmente detectará debilidades comunes o conocidas públicamente en el momento de la prueba, en lugar de buscar clases de vulnerabilidad nuevas o desconocidas anteriormente. Se deben utilizar probadores de penetración debidamente calificados. Por ejemplo, personas certificadas bajo los esquemas CHECK, CREST o Tiger.

Nota: Para obtener orientación sobre los riesgos de exponer la interfaz de gestión a diferentes redes, consulte el Principio 11 - Protección de la interfaz externa.

10. Identidad y autenticación

Todo acceso a las interfaces de servicio debe estar restringido a personas autenticadas y autorizadas.

Una autenticación débil de estas interfaces puede permitir el acceso no autorizado a sus sistemas, lo que puede resultar en el robo o modificación de sus datos, cambios en su servicio o una denegación de servicio.

Es importante que la autenticación se realice a través de canales seguros. El correo electrónico, HTTP o el teléfono son vulnerables a los ataques de interceptación y de ingeniería social.

Aspectos Clave - Identidad y autenticación

Debe tener confianza en que los controles de identidad y autenticación garantizan que los usuarios están autorizados a acceder a interfaces específicas.

Tips de Implementación - Identidad y autenticación

Aspecto	Descripción	Orientación
Autenticación de dos factores	Los usuarios se autentican con un nombre de usuario y un token de hardware/software, o un reto"fuera de banda" (por ejemplo, SMS).	Este enfoque se considera una buena práctica, suponiendo que se utilicen sistemas de autenticación estándar y bien probados.
Certificado de cliente TLS	El servicio admite la autenticación a través de TLS utilizando un certificado de cliente X.509v3 que identifica a un usuario individual.	Este método proporciona una fuerte protección criptográfica. Su fortaleza, sin embargo, depende de la creación y gestión segura de certificados y de las medidas de seguridad que se aplican a los dispositivos de los usuarios finales para protegerlos. Si un certificado de cliente es robado por el malware de un dispositivo, puede

		ser reutilizado por un atacante para obtener acceso al servicio; sólo un factor de autenticación adicional (véase más adelante) lo impediría. Se necesitarán procesos para revocar las credenciales perdidas o comprometidas.
Federación de identidad con su proveedor de identidad existente	El servicio soporta la federación a otro esquema de autenticación, como un directorio corporativo, un proveedor de OAuth o SAML.	El uso de enfoques de identidad federada puede proporcionarle la ventaja de tener que gestionar un único sistema de identidad y autorización, en lugar de muchos. Sin embargo, tenga cuidado de que las soluciones de identidad federadas adquieran los riesgos de la solución de identidad de origen. El compromiso de esa solución de identidad de origen dará acceso a cualquier recurso protegido por identidades federadas. Por ejemplo, una solución de identidad de origen basada únicamente en la autenticación de nombre de usuario y contraseña tendría los riesgos que se describen a continuación.
Acceso limitado a través de enlaces dedicados, redes empresariales o comunitarias	El acceso a un servicio está limitado a una red privada o comunitaria.	Este método por sí solo no es suficiente para proteger su servicio, pero puede ser utilizado además de otros métodos. En esos

		casos, reducirá la oportunidad de que un atacante aproveche las credenciales robadas, ya que también necesitaría tener acceso a la red de la empresa o de la comunidad para hacerlo. Las redes muy grandes deben ser tratadas normalmente como si fueran públicas.
Nombre de usuario y contraseña	La autenticación se realiza a través de un nombre de usuario y una contraseña básicos, sin que los consumidores del servicio puedan hacer cumplir la selección de contraseñas seguras.	Los nombres de usuario y las contraseñas pueden verse afectados por el phishing o el malware en los dispositivos de los usuarios finales. La falta de un segundo factor de autenticación significa que cualquier credencial comprometida puede ser reutilizada por un atacante para obtener acceso al servicio. Las credenciales pasadas a través de canales no cifrados corren un riesgo especial de interceptación, por lo que es importante enviarlas a través de conexiones cifradas.

Notas adicionales - Riesgos de autenticación

Los riesgos asociados con una cuenta de usuario comprometida variarán dependiendo de los privilegios otorgados a la cuenta. Las cuentas altamente privilegiadas, con acceso a grandes volúmenes de datos de usuario (o la capacidad de alterar la configuración y seguridad del servicio) son de alto valor potencial para un atacante. Una autenticación débil de estas cuentas privilegiadas es normalmente un riesgo mayor que el de los usuarios regulares del servicio.

Las contraseñas muy largas, los requisitos de complejidad o las frecuencias de cambio pueden aumentar las posibilidades de que los usuarios manejen mal las contraseñas, las almacenen de forma insegura, las compartan o las reutilicen. Las protecciones alternativas (como la autenticación de dos factores) suelen ser una mejor opción que las contraseñas muy largas.

El monitoreo y la protección activos pueden ser una valiosa mitigación contra los riesgos de autenticación. La obstaculización de los ataques de fuerza bruta mediante el bloqueo, el bloqueo o la limitación de la velocidad proporciona una mitigación útil y puede ayudar a la detección.

Proporcionar desencadenantes basados en el riesgo (como pedir que se vuelva a autenticar para realizar acciones importantes, o exigir información de autenticación adicional desde ubicaciones o dispositivos desconocidos) también puede ayudar a detectar y mitigar la amenaza de credenciales comprometidas.

11. Protección de la interfaz externa

Todas las interfaces externas o menos fiables del servicio deben ser identificadas y defendidas adecuadamente.

Si algunas de las interfaces expuestas son privadas (como las interfaces de gestión), el impacto del compromiso puede ser más significativo.

Puede utilizar diferentes modelos para conectarse a servicios cloud que exponen los sistemas de su empresa a diferentes niveles de riesgo.

Aspectos Clave - Protección de la interfaz externa

Deberas,

- Comprender de qué interfaces físicas y lógicas está disponible su información y cómo se controla el acceso a sus datos
- Tener la suficiente confianza de que el servicio identifica y autentica a los usuarios a un nivel apropiado a través de esas interfaces (véase el Principio 10 : Identidad y Autenticación)

Tips de Implementación - Protección de la interfaz externa

Los servicios pueden proteger sus datos limitando la oportunidad de un atacante de conectarse. Esto puede hacerse proporcionando el servicio sólo a un conjunto limitado de redes, ubicaciones o dispositivos.

Aspecto	Descripción	Orientación
Internet	Los usuarios se conectan al servicio directamente a través de Internet.	Dado que se puede acceder al servicio desde cualquier dispositivo conectado a Internet, los ataques se pueden lanzar desde cualquier lugar. Por lo tanto, es importante que el proveedor de servicios haya diseñado las interfaces externas de su servicio para que sean resistentes a los

		ataques. El proveedor del servicio debe disponer de un régimen de pruebas continuas para garantizar que todas las interfaces expuestas al público sigan siendo seguras.
Red comunitaria	Algunos servicios en la nube (en particular los servicios comunitarios en la nube) sólo pueden conectarse directamente a redes comunitarias privadas (por ejemplo, la Red de Servicios Públicos).	Si el servicio en la nube está dedicado a la comunidad y sólo es accesible a través de la red de la comunidad, es probable que el servicio esté menos expuesto a los atacantes remotos. Para que un atacante apunte a su conexión al servicio de nube, necesitaría tener acceso a la red de la comunidad, ya sea por ser parte de la comunidad o por haber comprometido a alguien que lo es.
Red privada	Algunos servicios pueden proporcionar conexiones dedicadas a su red.	Dependiendo del diseño del servicio, los atacantes que se dirigen a servicios en la nube sólo expuestos a redes privadas pueden verse obligados a comprometer primero una red privada. Sin embargo, si el servicio también ofrece conectividad a Internet, entonces también debe revisar la guía anterior.

Notas adicionales - Autenticación en interfaces externas

Los servicios accesibles a través de Internet, en particular los que aceptan conexiones desde cualquier lugar, están más expuestos a los ataques, por lo que será especialmente importante tener una gran confianza en la solidez de la autenticación y el control de acceso.

Principio 10 : Identidad y Autenticación detalla los enfoques comunes para la identificación y autenticación y explica los riesgos asociados con cada uno de ellos.

12. Administración de servicios seguros

Los sistemas utilizados para la administración de un servicio en la nube tendrán un acceso altamente privilegiado a ese servicio. Su compromiso tendría un impacto significativo, incluyendo los medios para eludir los controles de seguridad y robar o manipular grandes volúmenes de datos.

El diseño, la implementación y la gestión de los sistemas de administración deben seguir las buenas prácticas de la empresa, al tiempo que se reconoce su alto valor para los atacantes.

Aspectos Clave - Administración de servicios seguros

Deberías,

- Entender qué modelo de administración de servicios está utilizando el proveedor de servicios para gestionar el servicio
- Contentarse con los riesgos que el modelo de administración del servicio en uso conlleva para sus datos o el uso del servicio

Tips de Implementación - Administración de servicios seguros

Aspecto	Descripción	Orientación
Arquitectura de gestión de servicios desconocida	El proveedor del servicio no ha revelado esta información.	En este caso, sería prudente asumir que los riesgos asociados con el enfoque de *administración del servicio directo* están presentes.
Arquitectura de gestión de servicios conocida	El proveedor de servicios ha identificado qué modelo de administración de sistemas se utiliza para administrar el servicio.	Para comprender los riesgos asociados a los diferentes modelos de administración de sistemas, consulte el apartado modelo de administración de sistemas El nivel de seguridad que usted tiene de que las afirmaciones del proveedor de servicios son correctas puede variar. Puede obtener una garantía independiente

		de un arquitecto de seguridad debidamente cualificado.
Otros	El proveedor del servicio puede creer que su enfoque de administración de sistemas no está cubierto por uno de los modelos descritos en el apartado modelo de administración de sistemas	En este caso, le corresponderá a usted hacer su propia evaluación sobre los riesgos asociados con el enfoque de administración del proveedor de servicios.

Notas adicionales - Protección de los dispositivos de administración

Un aspecto importante de la seguridad de las interfaces de administración privilegiadas es la seguridad de los dispositivos de usuario final utilizados para la administración. Es importante que tanto usted como el proveedor de servicios se aseguren de que los dispositivos utilizados para actividades especialmente privilegiadas estén bien protegidos. Por ejemplo, no deben utilizarse para navegar directamente por la web o leer correo electrónico, ya que se trata de actividades de alto riesgo para que alguien las realice desde un dispositivo utilizado para la administración.

13. Información de auditoría para los usuarios

Se le deben proporcionar los registros de auditoría necesarios para supervisar el acceso a su servicio y los datos que contiene. El tipo de información de auditoría disponible para usted tendrá un impacto directo en su capacidad de detectar y responder a actividades inapropiadas o maliciosas dentro de plazos razonables.

Aspectos Clave - Información de auditoría para los usuarios

Deberías,

- Conocer la información de auditoría que se le proporcionará, cómo y cuándo estará disponible, el formato de los datos y el período de retención asociado con ellos
- Que la confianza de que la información de auditoría disponible satisfaga tus necesidades para investigar el uso indebido o los incidentes

Tips de Implementación - Información de auditoría para los usuarios

Aspecto	Descripción	Orientación
Ninguno	El proveedor de servicios no ofrece información de auditoría a los usuarios.	La falta de información de auditoría puede impedir que usted identifique el uso indebido de su servicio y de sus datos. Usted debe considerar si la incapacidad de determinar cómo, cuándo o dónde se accede a un servicio podría resultar en problemas legales o regulatorios.
Datos disponibles mediante negociación	El proveedor de servicios ofrece a los usuarios información de auditoría limitada como resultado de la negociación.	Debe considerar si los datos de auditoría proporcionados son adecuados para apoyar sus necesidades. El suministro de información de auditoría no le proporciona por sí mismo

		ninguna protección. La información requerirá un análisis para descubrir evidencia de compromiso o mal uso.
Datos disponibles	El proveedor del servicio pone a disposición de los usuarios datos de auditoría específicos. Se especifica el calendario, el método, el formato y el período de conservación de los datos.	Debe considerar si los datos de auditoría proporcionados son adecuados para apoyar sus necesidades. El suministro de información de auditoría no le proporciona por sí mismo ninguna protección. Para ello, la información requerirá un análisis que permita descubrir pruebas de compromiso o uso indebido.

Notas adicionales - Utilización de los datos de auditoría

Los datos de auditoría tienen un valor limitado a menos que se utilicen como parte de un régimen de supervisión eficaz. Un buen monitoreo requiere una comprensión completa del uso esperado del servicio.

Para los servicios IaaaS y PaaS, el proveedor de servicios o un tercero puede ofrecer servicios de supervisión de protección de valor añadido para las cargas de trabajo que haya implementado. Al considerar estos servicios, piense en el apoyo que el proveedor de servicios o un tercero necesitaría para prestar un servicio perspicaz.

Considere si requiere que los registros de auditoría se mantengan de acuerdo con normas específicas o si son adecuados para circunstancias específicas.

14. Uso seguro del servicio

La seguridad de los servicios en la nube y de los datos que contienen puede verse afectada si se utiliza mal el servicio. En consecuencia, usted tendrá ciertas responsabilidades al utilizar el servicio para que sus datos estén adecuadamente protegidos.

El alcance de su responsabilidad variará en función de los modelos de implementación del servicio cloud y del escenario en el que desee utilizar el servicio. Las características específicas de los servicios individuales también pueden ser relevantes. Por ejemplo, cómo una red de entrega de contenido protege su clave privada, o cómo un proveedor de pago en la nube detecta transacciones fraudulentas, son consideraciones de seguridad importantes más allá de las consideraciones generales cubiertas por los principios de seguridad de la nube.

Con las ofertas de IaaS y PaaS, usted es responsable de aspectos significativos de la seguridad de sus datos y cargas de trabajo. Ver apartado Responsabilidad Compartida. Por ejemplo, si adquiere una instancia de cálculo IaaS, normalmente será responsable de instalar un sistema operativo moderno, configurar ese sistema operativo de forma segura, desplegar de forma segura cualquier aplicación y también mantener esa instancia mediante la aplicación de parches o la realización del mantenimiento necesario.

Aspectos Clave - Uso seguro del servicio

Deberás,

- Comprender las opciones de configuración de servicios disponibles para usted y las implicaciones de seguridad de sus elecciones
- Entender los requisitos de seguridad de su uso del servicio
- Educar a su personal que utiliza y gestiona el servicio sobre cómo hacerlo de forma segura y protegida

Tips de Implementación - Uso seguro del servicio

Aspecto	Descripción	Orientación
Dispositivos gestionados por la empresa	Se accede al servicio desde dispositivos bajo su control	Un único dispositivo comprometido tendría acceso a cualquier dato, funcionalidad o credencial accesible a los usuarios autorizados de ese

		dispositivo. Sin embargo, como los dispositivos están bajo su control, puede configurarlos de forma segura.
Dispositivos gestionados por socios o partners	El servicio es accesible desde dispositivos que usted entienda la configuración de, o que tenga algún control sobre. Por ejemplo, mediante cláusulas contractuales o de conformidad con sus requisitos de seguridad.	Un solo dispositivo comprometido tendría acceso a cualquier dato, funcionalidad o credencial accesible a los usuarios autorizados de ese dispositivo, por lo que es importante asegurarse de que la configuración sea la adecuada. Si usted confía en contratos para hacer cumplir sus requisitos de seguridad con los socios, entonces deben estar bien redactados para asegurar que serán efectivos.
Dispositivos desconocidos	Usted tiene poco conocimiento de la configuración o estado de los dispositivos que acceden al servicio.	Es imposible para usted identificar los dispositivos comprometidos, por lo que debe asumir que un porcentaje distinto de cero de los dispositivos se verá comprometido.

Notas adicionales - Dispositivos del usuario final que se conectan al servicio

Además de los riesgos para el servicio en la nube, todo lo que construya sobre el servicio y sus datos, debe tener en cuenta los riesgos relacionados con las redes de su empresa y los dispositivos de usuario final conectados al servicio.

Para algunos de sus datos y cargas de trabajo puede ser apropiado requerir el uso de dispositivos administrados y emitidos por la empresa con una configuración adecuada para garantizar la seguridad suficiente. Los riesgos asociados a las diferentes opciones se describen en la tabla anterior.

Separación y seguridad en la nube

Modelos de implementación y modelos de servicio

Al evaluar las medidas de separación de un servicio en la nube dado, hay dos factores que determinan sus requisitos de seguridad y garantía: el modelo de implementación y el modelo de servicio.

Hemos aislado tres modelos de implementación: implementaciones de nube pública, nube comunitaria y nube privada.

Y tres modelos de servicio: Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS).

Primero veremos los modelos de implementación, luego pasaremos a considerar los requisitos de separación de los diversos modelos de servicio. La sección final resume los riesgos asociados con cada uno de los modelos de servicio.

Modelos de separación e Implementación

Nube pública

Normalmente, cualquier persona que posea una tarjeta de crédito puede acceder a los servicios en la nube pública. Para algunos servicios, una dirección de correo electrónico es todo lo que se requiere para acceder a las versiones de prueba gratuitas.

Por lo tanto, si está utilizando el servicio de nube pública, debe aceptar que sus adversarios puedan comprar legítimamente un servicio "al lado" del suyo.

En tales casos, probablemente desee un alto nivel de confianza en los controles que separan sus datos de los de otros.

Nube de la comunidad

Los servicios en la nube de la comunidad alojan usuarios de una comunidad específica, como el sector público.

Estas comunidades a menudo tienen un apetito de riesgo compartido y generalmente esperan que los miembros cumplan con un estándar mínimo acordado o un acuerdo legal.

Los proveedores de la nube comunitaria a menudo pueden adaptar sus ofertas para que coincidan con los requisitos de la comunidad. Por ejemplo, un proveedor de servicios podría elegir cumplir con los estándares específicos del gobierno del Reino Unido para el control de seguridad del personal, o cumplir con el estándar requerido para conectarse a una red

comunitaria del gobierno. Estas ofertas personalizadas a veces pueden reducir los riesgos relacionados con uno o más de los principios de seguridad en la nube.

Dedicar un servicio a una sola comunidad (donde existe confianza entre los miembros de esa comunidad) reduce los riesgos asociados con la separación entre usuarios.

El nivel de confianza entre los usuarios dependerá de los estándares que los miembros de la comunidad están obligados a cumplir. Junto con los tipos de aplicaciones implementadas, este nivel de confianza determinará si un servicio en la nube de la comunidad cumple con los controles de separación requeridos.

Nube privada

Los servicios de nube privada se implementan para admitir una sola organización. Normalmente ofrecen la capacidad de adaptar la arquitectura para cumplir con los requisitos específicos de seguridad y comerciales. Por ejemplo, si todos los consumidores del servicio son bien conocidos y de bajo riesgo, entonces el nivel de garantía de separación requerido puede ser bajo.

Para procesar datos no confiables (posiblemente maliciosos) o muy confidenciales, puede requerir una mayor confianza en los controles de separación. Deberá administrar, monitorear y mantener la infraestructura, a menos que exista un acuerdo con el proveedor de servicios en la nube para hacerlo.

En muchas situaciones, un servicio de nube privada operará dentro de un único dominio de seguridad (por ejemplo, proporcionando un escritorio virtual o recursos de prueba y desarrollo). En tales escenarios, la plataforma en la nube es simplemente otra parte del entorno de TI empresarial y debe configurarse, administrarse y monitorearse como tal.

Los controles de seguridad en entornos de nube privada normalmente no necesitan altos niveles de seguridad, a menos que tenga requisitos de seguridad particularmente desafiantes

Modelos de separación y servicio en la nube

Los controles técnicos necesarios para proporcionar la separación variarán según el modelo de servicio empleado. Los consideraremos para cada tipo de servicio por turno.

Infraestructura como servicio (IaaS)

Los productos IaaS generalmente brindan servicios de cómputo, redes y almacenamiento. La separación del usuario debe hacerse cumplir en todos estos elementos.

IaaS: separación de cómputo

Dentro del entorno de cómputo, la separación entre usuarios generalmente se aplica mediante un hipervisor (aunque en algunas circunstancias también se puede lograr mediante la asignación de hardware físico a los consumidores).

La fuerza de la separación generalmente depende de la tecnología de virtualización en uso. El uso de la virtualización de hardware y los productos de virtualización garantizados deberían proporcionar una mayor confianza en la separación dentro del entorno informático. Obviamente, esto depende de la configuración y el funcionamiento correctos del producto.

Las herramientas de administración que soportan el producto de virtualización también deben estar aseguradas, ya que son fundamentales para la seguridad que brinda el producto.

IaaS: separación de red

Es importante comprender el modelo de separación de red de una oferta de IaaS, ya que los usuarios normalmente construirán sus propias redes virtuales en una infraestructura de red multicliente.

El proveedor de servicios podría utilizar una serie de tecnologías para forzar la separación de la red. Estos incluyen el uso de LAN virtuales (VLAN), tecnologías de enrutamiento y reenvío virtuales (VRF) o capacidades de red virtual dentro del entorno informático.

Si no puede obtener suficiente confianza en la separación proporcionada por un servicio IaaS dentro de la capa de red, puede mejorar su protección de confidencialidad con su propio cifrado. Esto se describe en nuestra guía de configuración de IaaS.

También es posible que deba considerar si el servicio protege o reserva su parte de los recursos de la red, de modo que un ataque (como un DDoS) a otro usuario no afecte la provisión de su servicio.

IaaS: almacenamiento

En un modelo IaaS, los usuarios pueden tener control directo sobre una parte de un entorno de almacenamiento multiempresa. Proporcionar a los usuarios este control directo hace posible que un usuario malintencionado o comprometido ataque los componentes de almacenamiento del servicio para obtener acceso a los datos de otro usuario. La separación efectiva dentro del almacenamiento del servicio ayudará a abordar este problema.

Los usuarios de IaaS pueden reducir su dependencia de la separación de almacenamiento del proveedor de servicios en la nube cifrando sus propios datos. Esto presenta sus propios desafíos, y solo será efectivo si las claves de cifrado para los datos se pueden almacenar de tal manera que no sean accesibles para un atacante que tenga acceso al almacenamiento.

Plataforma como servicio (PaaS)

Las ofertas de PaaS pueden proporcionar a los usuarios interfaces ricas y complejas. Cubren una amplia gama de tecnologías de implementación y es probable que se encuentren en diferentes niveles de madurez de seguridad.

Dependiendo de las tecnologías involucradas, puede ser difícil, lento y costoso obtener altos niveles de seguridad en la separación proporcionada por una oferta de PaaS.

Las aplicaciones que desean mayor seguridad en la separación proporcionada por una oferta de PaaS pueden, en cambio, basarse en una oferta de IaaS que tenga suficiente seguridad de tal manera que IaaS subyacente haga cumplir la separación. Alternativamente, puede ser apropiado ejecutar la solución PaaS dentro de un servicio en la nube privado o comunitario.

A continuación se describen dos enfoques comunes de PaaS, con diferentes riesgos asociados.

Hosting de aplicaciones compartidas

Un modelo común de PaaS, particularmente para la entrega de alojamiento de aplicaciones web, implica el alojamiento de aplicaciones de los usuarios sobre un sistema operativo compartido. En este modelo, el sistema operativo y el host de la aplicación (por ejemplo, el servidor web y el host de secuencias de comandos o el tiempo de ejecución) son responsables de evitar que los usuarios se afecten entre sí.

Si los atacantes pueden ejecutar legítimamente una aplicación en el mismo host, tienen acceso a una gran superficie de ataque para intentar escalar privilegios y obtener acceso no autorizado.

Servicios de host gestionados

Otro modelo común de PaaS es la provisión de servicios de sistema operativo administrado. En este modelo, el usuario tiene una máquina física o virtual dedicada, pero en lugar de administrar el sistema operativo por sí mismo, lo compra como un servicio del proveedor de servicios.

Los riesgos en este modelo son muy similares a los de un servicio IaaS, ya que es probable que la aplicación de la separación se base en la misma tecnología subyacente (generalmente un hipervisor).

Hay dos riesgos adicionales clave (en comparación con un servicio IaaS equivalente) a tener en cuenta al considerar la idoneidad de este modelo:

Los administradores del proveedor de servicios tendrán acceso privilegiado al sistema operativo. Esto significa que es más fácil para ellos acceder a sus datos que si solo tuvieran acceso a imágenes de disco.
Al proporcionar el servicio de administración, es probable que haya conexiones adicionales entre sus máquinas y la infraestructura de administración. Esta infraestructura es un vector de ataque adicional en comparación con el caso simple de IaaS.

Software como servicio (SaaS)

En las ofertas de SaaS, la separación entre usuarios a menudo se impone mediante controles de software que se ejecutan dentro de una sola instancia de una aplicación. La fuerza de la separación depende de la arquitectura y la implementación de la aplicación.

Por lo general, no se confía en la plataforma y la infraestructura subyacentes para forzar la separación, lo que dificulta obtener altos grados de confianza en la fuerza de la separación. En las ofertas de SaaS puede ser difícil entender dónde y cómo se protegen sus datos.

Algunas ofertas de SaaS pueden estar dedicadas a un solo consumidor, aprovechando los controles de una solución IaaS o PaaS para brindar a los usuarios confianza en la separación de sus datos.

En las ofertas de SaaS, el proveedor de servicios generalmente dependerá de los controles de nivel de aplicación en lugar de los controles en la infraestructura o plataforma, lo que significa que si un componente del servicio se ve comprometido, los datos de muchos usuarios pueden ser visibles para ese componente.

Si necesita más seguridad en la separación proporcionada por una oferta de SaaS, es posible que desee aprovechar una oferta de IaaS o PaaS que tenga suficiente seguridad en los controles de separación subyacentes. Alternativamente, puede ser apropiado ejecutar la solución SaaS dentro de un servicio en la nube privado o comunitario.

Riesgos asociados con los modelos de servicio.

La siguiente tabla resume los principales riesgos asociados con cada uno de los modelos de servicio

Modelo de servicio	Riesgos asociados
Infraestructura como servicio (IaaS)	Las ofertas implementadas mediante virtualización de hardware y productos de virtualización líderes pueden proporcionar un buen nivel de separación entre las cargas de

	trabajo y los datos en las plataformas de nube pública y comunitaria. Sin embargo, como todo el software complejo, las ofertas de IaaS nunca estarán libres de vulnerabilidades y los riesgos que conllevan. Los servicios de IaaS también tienen una carga mucho mayor sobre el usuario para configurar y operar bien
Plataforma como servicio (PaaS)	Las ofertas de PaaS tienden a tener una superficie de ataque mayor que las ofertas de IaaS, ya que la separación entre usuarios normalmente se proporciona en un software de nivel superior en lugar de un hipervisor. Las ofertas de PaaS en la nube comunitaria pueden proporcionar cierta comodidad adicional para los usuarios cuando existe una política de uso aceptable diseñada para reducir el riesgo de cargas de trabajo maliciosas. Las tecnologías PaaS están evolucionando rápidamente y debe verificar regularmente que su elección de plataforma satisfaga sus necesidades comerciales y de seguridad.
Software como servicio (SaaS)	Las ofertas de SaaS tienden a implementar la separación a un nivel más alto que IaaS y PaaS, lo que significa que la superficie de ataque potencial para un posible atacante es mucho mayor. A menos que estén bien diseñados, estos servicios a menudo presentan un riesgo potencialmente mayor que la implementación de paquetes de software para un usuario dedicado dentro de un servicio IaaS o PaaS.

Responsabilidad Compartida en la Gestión de la Seguridad en infraestructura

Responsabilidad Compartida

Proveedores y Clientes deben actuar bajo un esquema de responsabilidad compartida sobre la seguridad de los servicios de la siguiente forma:

Responsabilidad del Proveedor sobre Servicios IaaS

El Proveedor es responsable de la infraestructura que soporta los servicios IaaS que abarca la infraestructura de red, de procesamiento, de almacenamiento, la capa de virtualización de los servicios. El Porveedor , debe garantizar la seguridad física y lógica de los centros de datos ante ataques de denegación de servicio y vulnerabilidades de hardware y software sobre su infraestructura incluyendo el mantenimiento de actualizaciones de seguridad de la capa de virtualización.

Responsabilidad del Proveedor sobre Servicios PaaS

El Proveedor es responsable de la plataforma de servicios que abarca la infraestructura de red, de procesamiento, de almacenamiento, la capa de virtualización de los servicios, sistema operativo y plataforma de servicios. El Proveedor , debe garantizar la seguridad física y lógica de los centros de datos ante ataques de denegación de servicio y vulnerabilidades de hardware y software de la plataforma y el mantenimiento de actualizaciones e seguridad de la plataforma.

Responsabilidad del Cliente

El Cliente es responsable de (i) el software (incluyendo la actualización de SO si es IaaS) , aplicaciones y datos que instale sobre los recursos entregados por el Proveedor, (ii) diseñar la arquitectura de seguridad de la información para protegerla de amenazas y vulnerabilidades cibernéticas, (iii) gestionar el tratamiento y el contenido de la información, (iv) establecer las políticas de gestión de seguridad de la información, de la gestión de los usuarios y configuración de permisos de acceso a los recursos contratados.

Arquitecturas de administración de sistemas

Existen varios modelos arquitectónicos diferentes que se pueden usar para diseñar el enfoque de administración para los sistemas de TI. Esta sección describe algunos enfoques comunes y los riesgos asociados con cada uno.

Modelos de administración

Algunos modelos conllevan mucho más riesgo que otros, y se desaconseja su uso. Los enfoques más inseguros se identifican con el siguiente símbolo !!!

Modelo de administración	Descripción	Riesgo asociado
Dispositivos dedicados en una red segregada.	El servicio se administra desde dispositivos dedicados en una red de administración segregada. Los dispositivos son únicamente para la gestión de servicios y no para uso general, como el correo electrónico y la navegación web.	Con este enfoque, los dispositivos de administración y la red segregada son difíciles de atacar. Este enfoque también puede ayudar a apoyar las medidas de seguridad del personal para sistemas de mayor seguridad. Por ejemplo, cuando el proveedor de servicios desea demostrar que solo el personal que ha sido sometido a estrictos controles de seguridad (o que posee las autorizaciones de seguridad apropiadas) tiene acceso a las funciones de administración del sistema.
Dispositivos dedicados para la administración de servicios comunitarios.	Los dispositivos están dedicados a la gestión de servicios para una sola comunidad (por ejemplo, sector público del Reino Unido). La red de gestión está segregada de todas las demás redes.	Cuando se administran múltiples servicios, existe el riesgo de que un servicio más vulnerable pueda verse comprometido y utilizado como plataforma provisional para atacar la red de administración. La gestión conjunta de servicios con

	Los dispositivos se utilizan únicamente para la gestión de servicios y no para uso general, como el correo electrónico y la navegación web.	posturas de seguridad similares ayudará a reducir este riesgo. Este enfoque también puede ayudar a apoyar las medidas de seguridad del personal para sistemas de mayor seguridad. Por ejemplo, cuando el proveedor de servicios desea demostrar que solo el personal que ha sido sometido a estrictos controles de seguridad (o que posee las autorizaciones de seguridad apropiadas) tiene acceso a las funciones de administración del sistema.
Dispositivos dedicados para la administración de múltiples servicios comunitarios.	Los dispositivos están dedicados a la administración de servicios, pero se usan para administrar múltiples servicios en múltiples comunidades de usuarios. Los dispositivos se utilizan únicamente para la gestión de servicios y no para uso general, como el correo electrónico y la navegación web.	En este modelo, los dispositivos en sí mismos siguen siendo objetivos difíciles de atacar, pero el alcance más amplio y amplio de la red de administración puede hacer que esté más expuesto a los ataques.
Administración de servicios a través de hosts bastion !!!	Este modelo (también conocido como "exploración") es donde un servicio se administra utilizando dispositivos de una red menos confiable (como una red empresarial corporativa), pero solo por personal de administración autorizado. Ese personal tiene acceso a hosts de administración específicos,	Los sistemas corporativos tienden a procesar una amplia gama de tipos de contenido y son más vulnerables a los ataques utilizando técnicas típicas. Los hosts de bastión brindan cierta protección contra las amenazas de las redes corporativas, pero es probable que los atacantes

	conocidos como bastiones, desde los cuales se llevan a cabo todas las acciones de administración en el servicio.	con acceso a dispositivos corporativos utilizados por los administradores de servicios aún puedan acceder al entorno de administración de servicios como si fueran administradores legítimos. El malware capaz de realizar secuestros de sesiones se está volviendo cada vez más común, por lo que los riesgos asociados con este modelo también están aumentando.
Administración directa del servicio !!!	El servicio se administra directamente desde dispositivos que también se usan para negocios normales (navegación web, visualización de correo electrónico externo, etc.)	En este modelo, hay poca protección del servicio contra el acceso no autorizado a las interfaces de administración. Los servicios gestionados de esta manera tienen un riesgo significativo de compromiso.