Medidas de Seguridad en entornos Cloud

CTEAJE
Comité Técnico Estatal de la
Administración Judicial Electrónica

Ficha del Documento

GRUPO DE TRABAJO	Subcomité de Seguridad. Línea de Trabajo CLOUD
NOMBRE DEL DOCUMENTO	Medidas de Seguridad en entornos Cloud
CÓDIGO DEL DOCUMENTO	Haga clic para escribir texto
VERSIÓN	V1.0

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
V0.1	Oficina de Gobierno de Ciberseguridad	13/06/2024	Versión inicial del documento.
V0.2	Oficina de Gobierno de Ciberseguridad	27/09/2024	Actualización del documento que completa medidas de seguridad para logs y backups e incorpora recomendaciones de seguridad desde la perspectiva de Arquitectura y estrategia Cloud (aportaciones del Ministerio). Se alinea la ubicación de servidores e infraestructura con el posicionamiento que establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (artículo 46 bis) para sectores públicos esenciales.
V0.3	Oficina de Gobierno de Ciberseguridad	17/10/2024	Se completan medidas de seguridad relacionadas con los siguientes aspectos: • Custodia de los logs • Custodia de los backups • SIEM SaaS • BCP y DRP
V1.0	Oficina de Gobierno de Ciberseguridad	24/10/2024	Versión resultante de la Línea de Trabajo Cloud. Versión aprobada en Subcomité de Seguridad de fecha 24 de octubre de 2024.
V1.0	Oficina de Gobierno de Ciberseguridad	26/02/2025	Versión aprobada en CP 26/02/2025

Índice

1. OBJETO

En el ámbito de la Administración de Justicia resulta de especial interés elaborar una estrategia común, a nivel CTEAJE, en cuanto a la unificación de criterios en la contratación y uso de los servicios y los sistemas en los entornos Cloud.

El presente documento tiene por objeto el establecimiento de medidas y requisitos mínimos de seguridad y privacidad para:

- Tratamientos de datos y servicios de Justicia en entornos Cloud

Estos requisitos mínimos se establecen, sin perjuicio de la aplicación del resto de medidas exigibles a los sistemas de información del ENS/EJIS, en función de su categoría y valoración, y de la normativa de protección de datos, con el objeto de ayudar a identificar los requisitos de seguridad a solicitar al proveedor de servicios en la nube, para su inclusión en las condiciones contractuales, y delimitar responsabilidades y obligaciones (Proveedor / Administración).

2. MEDIDAS DE SEGURIDAD DE SERVICIOS EN ENTORNOS CLOUD

Estas medidas aplican a toda aquella información que pueda ser tratada y/o almacenada a través de servicios en entornos Cloud externos y puestos a disposición por la Administraciones prestacionales en sus diferentes modalidades: IaaS (infraestructura como servicio), PaaS (plataforma como servicio) o SaaS (software como servicio).

Conformidad con el ENS

- Conformidad con el ENS de la infraestructura que ejecuta todos los servicios provistos en Cloud o del proveedor de servicios Cloud (CSP), en la categoría y niveles requeridos por la administración prestacional:
  - Asegurar que los servicios en los que está interesada la administración están incluidos en el **alcance** del Certificado de Conformidad con el ENS del CSP.
  - Asegurar que se contratan, al menos, los servicios necesarios del **catálogo** para cumplir con el ENS (por ejemplo, la elección de dos CPD en diferentes zonas para la prestación del servicio Cloud, junto a la opción de replicación entre ambos a efectos de disponibilidad).
  - Si el servicio Cloud dispone de un **Perfil de Cumplimiento Especifico**, la Administración prestacional deberá seguir y aplicar las pautas descritas en las **Guías de configuración segura** establecidas.
  - En caso de que no disponga de Perfil de Cumplimiento Especifico, o que no pueda ser aplicado, el CSP deberá proveer información (guía de configuración o similar) sobre los procedimientos y mecanismos para el cumplimiento de las distintas medidas de seguridad aplicables.

- Establecer claramente el **modelo de responsabilidad compartida** con el CSP, considerando toda la cadena de suministro, en cuanto al cumplimiento de las medidas de seguridad y privacidad exigibles tal y como se exige el ENS.
  - Acuerdos de nivel de servicio, que regirán la calidad del servicio Cloud contratado, reflejando aspectos relativos a capacidad, disponibilidad, continuidad o relativos a la gestión de incidentes, peticiones de cambio, entre otros.

Cumplimiento de la normativa de protección de datos *(en caso de que el servicio Cloud suponga tratamiento de datos de carácter personal)*

- Formalización de **contrato de encargo** de tratamiento.
  - Compromiso por parte del CSP a mantener la **confidencialidad** en el tratamiento de la información de los sistemas que provee a la Administración prestacional, y a no divulgar o acceder indebidamente a la información.
  - El CSP queda obligado a no acceder ni utilizar la información a la que tenga acceso para fin alguno que no esté explicitado en el contrato o se autorice expresamente por escrito con posterioridad a la firma del contrato.
- Los sistemas de información y comunicaciones, así como la infraestructura, que sostienen los servicios Cloud, y que traten datos de la Administración de Justicia, incluidos los datos personales, deberán ubicarse y prestarse dentro del territorio del **Espacio Económico Europeo**. Los datos no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.
  - La Administración prestacional debe poder determinar dónde se almacenarán sus datos, incluida la región geográfica del almacenamiento.
- Se deberá valorar la obligación de realizar una **Evaluación de Impacto en Protección de Datos** (EIPD) antes de contratar servicios Cloud, y en todo caso, antes de iniciar un tratamiento de datos en entornos Cloud. En los sistemas de la Administración de Justicia es común la existencia de tratamientos de alto riesgo, asimismo de acuerdo con la lista de la AEPD[1] de tratamientos que requieren la realización de una EIPD:
  - *4. Tratamientos que impliquen el uso de **categorías especiales de datos** a las que se refiere el artículo 9.1 del RGPD, datos relativos a **condenas o infracciones penales** a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.*
  - *7. Tratamientos que impliquen el uso de datos a **gran escala**.*
  - *9. Tratamientos de datos de **sujetos vulnerables o en riesgo de exclusión social**, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y*

1 https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

- **Finalización del contrato**: regular los aspectos relativos a la devolución de la información, en cuanto al formato de los datos, así como los plazos. O en su defecto, los relativos a la destrucción de la misma o al borrado seguro de la información almacenada por el CSP, requiriendo evidencias (certificados) de su realización.

Gobierno de las identidades y accesos

- Los datos de identidades se deberán mantener en la infraestructura de la Administración prestacional (**Gestión de Identidades y Accesos corporativo**). En caso de no ser posible, se deberá justificar y autorizar.
- La autenticación de los servicios Cloud se deberá realizar a través del Gestor de Identidades y Accesos corporativo (IAM) de la Administración prestacional. En caso de no ser posible, se deberá justificar y autorizar.
- Para la autenticación de los servicios Cloud se exigirá **doble factor de autenticación**.
- Si la gestión de los usuarios y accesos se realiza con recursos Cloud, requerir al CSP información detallada de cómo se realiza la gestión de los usuarios, control de acceso, política de contraseñas, cifrado, etc. El proveedor debe demostrar que los controles implantados son efectivos y funcionan correctamente, ya sea mediante renovación de certificaciones, auditorías periódicas o informes respecto a los controles aplicados.
- La Administración prestacional debe poder gestionar el acceso a sus datos y a los servicios y recursos del CSP a través de los usuarios, grupos, permisos y credenciales que quedan bajo su control.

Registros de actividad y logs

- Establecer la responsabilidad sobre los registros de actividad, estableciendo obligaciones en cuanto a su **configuración**, la consolidación periódica de datos, la **retención** de los registros y respecto a los mecanismos implementados para la **protección** de dichos registros.
- El CSP deberá permitir a la Administración prestacional el acceso y análisis de los diferentes registros de acceso y logs, y cualquier otra información que pudiera ser solicitada para garantizar el cumplimiento de las obligaciones legales.
  - **Periodicidad de sincronización** de logs:
    - Recolección en tiempo real o cercana al tiempo real: los logs se deberán sincronizar en intervalos cortos de tiempo, preferiblemente en tiempo real o con una latencia mínima determinada por cada Administración.
  - **Almacenamiento y custodia** de logs en entornos Cloud:
    - Centralización de logs: centralizar todos los logs en una ubicación confiable y segura. Utilizar un bucket cifrado en la nube o un sistema de archivos seguro que cumpla con los niveles de seguridad requeridos del ENS.

- Mantener la integridad de los logs utilizando mecanismos de protección contra cambios y borrados (WORM, write-once-read-many), así como aplicar cifrado en tránsito y reposo.
- Definir el período de retención de los logs, y limitar el acceso a personal debidamente autorizado, aplicando medidas de IAM.
- Asegurar que los logs se almacenen en múltiples ubicaciones físicas y regiones geográficas. Idealmente, utilizar almacenamiento en Cloud con replicación automática en diferentes zonas de disponibilidad.
- Implementar sistemas que monitoricen en tiempo real los eventos generados y alerten automáticamente de comportamientos anómalos en los logs.

- **Integración con el SIEM**: los logs deben ser enviados directamente a un SIEM centralizado, ya sea local o en la nube, para su análisis automatizado.
  - En el caso de que el **SIEM sea un servicio SaaS:**
    - Se ha de asegurar que la transferencia de datos al SIEM SaaS se realice mediante conexiones seguras y cifradas (TLS).
    - Se debe garantizar que la Administración mantenga el control sobre las políticas de retención y eliminación de los datos.
    - También se deben supervisar los accesos de manera continua y auditar las acciones realizadas, aplicando principios de mínimo privilegio. Se debe tener un plan de contingencia en caso de fallo del servicio SaaS y realizar revisiones de seguridad periódicas, incluyendo pruebas de vulnerabilidad y pentesting.

Gestión de incidentes y gestión de cambios

- Establecer los flujos de información y responsables de la gestión con el CSP para garantizar la fluidez en las comunicaciones y el cumplimiento de los plazos establecidos por la normativa de protección de datos.
- En caso de incidente de seguridad, toda la información requerida (configuración, logs, etc.) de los equipos físicos, dispositivos de red, servicios compartidos y dispositivos de seguridad debe ser entregada a la Administración prestacional.

Backup, recuperación de datos y BCP

- Establecer la responsabilidad sobre la realización de las copias de backup y la continuidad del servicio.
- Requerir al CSP la política de backup y recuperación de los datos, con el testeo periódico de los mecanismos de recuperación.
  - Disponer de un proceso automático de backup y garantizar que la frecuencia de los backups está alineada con el Punto Objetivo de Recuperación (RPO), o

cantidad máxima de información que puede ser perdida cuando el servicio es restaurado tras una interrupción, y que el tiempo de recuperación está alineado con el Tiempo Objetivo de Recuperación (RTO) del servicio, o tiempo límite para que el servicio vuelva a estar en funcionamiento.

- **Custodia en infraestructuras seguras**: garantizar que se custodian los backups en un repositorio diferente al original, es decir, almacenamiento en múltiples ubicaciones dentro del EEE. Puede ser tanto en la nube como en una infraestructura local o privada (en modelos híbridos); puede realizarse mediante técnicas de geo-replicación entre diferentes regiones o centros de datos.
- Establecer política que especifique la **duración del almacenamiento** de backups. Además, garantizar que los backups antiguos sean eliminados de manera segura, que no permita la recuperación del contenido (por ejemplo, mediante borrado criptográfico o destrucción física si es en soportes externos).
- Realizar **pruebas periódicas de restauración** de los backups. Las pruebas deben formar parte de un plan de recuperación de desastres más amplio.

- Para servicios Cloud que requieran una disponibilidad alta, requerir al CSP el plan de continuidad definido, con la verificación periódica de su correcta aplicación. Este plan de continuidad de negocio (BCP) ha de abordar los siguientes puntos:
  - Llevar a cabo un análisis de impacto en el negocio (BIA) para identificar los procesos críticos, definiendo objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO).
  - Asegurar **redundancia** de la infraestructura y los backups, así como la recuperación automática. Además, se han de realizar pruebas regulares del plan.
  - **Monitorización** proactiva que genere alertas sobre fallos en servicios esenciales y definir los procedimientos para activar el plan de contingencia en caso de desastre, incluyendo roles y responsabilidades de los equipos involucrados.

Cifrado de la información

- Toda la información de la Administración de Justicia que tenga establecidos requisitos de confidencialidad deberá encontrarse **cifrada** en la nube, tanto **en reposo**, considerando bases de datos o contenedores de documentos, como **en tránsito**.

Gestión de claves criptográficas

- No se almacenarán claves criptográficas en la nube, la Administración prestacional se encargará de la gestión y almacenamiento de las claves en su infraestructura. En caso de no ser posible, se deberá justificar y autorizar, siempre que se garantice que se almacenan por el proveedor de servicios Cloud (CSP) a través de módulos de seguridad de hardware o **dispositivo HSM** (Hardware Security Modules) **cualificados por el CCN.**

3. ANEXO - RECOMENDACIONES CLOUD

Las siguientes recomendaciones generales a nivel de arquitectura y estrategia Cloud deben ajustarse a la estrategia Cloud específica de cada Administración. Para brindar recomendaciones específicas, es esencial profundizar en aspectos clave como el modelo de despliegue (Cloud Pública, Privada, Híbrida, Multicloud), el modelo de servicio (IaaS, PaaS, CaaS, FaaS, SaaS), los principios estratégicos de arquitectura (Cloud Last, hacia on-prem, hacia Cloud, Cloud First, etc.), así como las preferencias y necesidades relacionadas con la migración.

Se han identificado seis áreas fundamentales para estas recomendaciones: **gobierno, usuarios e identidades, integración, seguridad de datos, plataformas y aplicaciones, e infraestructura Cloud.**

3.1 GOBIERNO

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones Estrategia Cloud
3.1.1 Definición de procesos y políticas	**Zero Trust en Accesos Cloud:** Implementar un marco de Zero Trust donde cada acceso a recursos Cloud esté basado en el principio de "Nunca confiar, siempre verificar". **Políticas Universales en Modelos Cloud Híbrida y MultiCloud:** Para modelos Cloud Híbrida y MultiCloud, definir políticas consistentes y universales que permitan gestionar accesos y auditorías centralizadas a través de todas las Clouds y entornos on-premise. **Controles en Redes, Almacenamiento y Cómputo para IaaS y PaaS:** Para entornos IaaS y PaaS, las políticas deben incluir controles sobre redes, almacenamiento y cómputo.	**Cloud Pública:** Funcionalidades de seguridad integradas y auditables en toda la infraestructura. **Cloud Híbrida**: Controles de seguridad coherentes en ambos entornos. **Cloud Privada**: Implementar políticas de seguridad avanzadas en redes, almacenamiento y cómputo. **IaaS/PaaS:** Controles de seguridad integrados en redes, almacenamiento y cómputo, con auditoría continua. **SaaS**: Asegurar que las aplicaciones gestionadas tengan controles de seguridad avanzados e integrados en cada capa. **Preferente Migrar:** Aquellas aplicaciones que requieren funcionalidades de seguridad avanzadas y auditables en tiempo real.

	Protección de Datos y Acceso en SaaS: Los entornos SaaS requieren políticas específicas para la protección de datos y acceso. **Seguridad Basada en el Riesgo:** Implementar herramientas que automaticen la identificación de riesgos en función del comportamiento de usuarios y sistemas, ajustando las políticas en tiempo real.	**Cloud First** para nuevas aplicaciones críticas que requieran seguridad avanzada integrada en toda la infraestructura. **Cloud Last**: En un entorno Cloud Last, las políticas deben enfocarse más en la infraestructura on-premise, asegurando que cualquier acceso desde Cloud esté restringido por políticas seguras. **Prohibir la subida de información clasificada de nivel superior a difusión limitada a la Cloud Pública.** Se debe usar Cloud Privada o Cloud Híbrida para información clasificada con nivel ALTO en las dimensiones de Confidencialidad (C), Integridad (I), Disponibilidad (A) y Trazabilidad (T). [ENS - Anexo II: Medidas de Seguridad]
3.1.2 Conformidad con el ENS	**Cumplimiento del ENS (Esquema Nacional de Seguridad):** Cumplir con las directrices del ENS, estableciendo políticas de auditoría, protección de datos y control de accesos para cada nivel de protección. **Auditoría Continua en Cloud Pública e Híbrida** En entornos Cloud Pública e Híbrida, es crucial implementar herramientas de auditoría continua que garanticen la conformidad en cada capa de la arquitectura**.** **Controles de Cumplimiento en SaaS:** Para servicios SaaS, utilizar controles de cumplimiento nativos que permitan auditorías continuas y reportes para la conformidad ENS.	**Cloud Pública**: Aprovechar auditorías automáticas para conformidad ENS. **Cloud Híbrida:** Implementar controles de cumplimiento en ambos entornos, asegurando coherencia en políticas**.** **Cloud Privada:** Mayor control sobre auditorías, con foco en conformidad estricta en sectores regulados. **SaaS**: Auditorías continuas en aplicaciones gestionadas. **IaaS/PaaS:** Conformidad en la configuración de recursos, redes y datos. **CaaS:** Asegurar auditorías sobre los contenedores.

	Servicios de Auditoría en IaaS y PaaS: En IaaS y PaaS, utilizar servicios de auditoría que monitoreen configuraciones de red, almacenamiento y cómputo. **Ajuste de Políticas Basadas en el Riesgo:** Ajustar las políticas de conformidad con base en los riesgos identificados.	**Preferente Migrar** servicios que requieren auditorías automáticas y conformidad continua. **Preferente No Migrar** si la aplicación ya cumple con ENS y no requiere grandes cambios.
3.1.3 Cumplimiento de la normativa de protección de datos	**Protección de Datos End-to-End en Multicloud y Híbrida:** Implementar un enfoque End-to-End para la protección de datos en Multicloud y Cloud Híbrida, asegurando que los datos estén protegidos en todas las fases: en tránsito, en reposo y en uso. Utilizar DLP para monitorizar y proteger datos sensibles. **Cifrado de Datos en Cloud Pública:** En Cloud Pública, los datos deben cifrarse utilizando HSMs o KMS nativos para asegurar la conformidad con la RGPD y otras normativas locales. **Controles Granulares en IaaS:** En el caso de IaaS, la arquitectura debe incluir controles granulares sobre los recursos de almacenamiento y bases de datos para evitar fugas de información. **Control de Datos en Cloud Privada:** En Cloud Privada, los controles deben centrarse en garantizar que los datos nunca salgan del entorno seguro sin autorización. **Implementar estructuras single-tenant para aplicaciones críticas:** Aplicaciones que requieran	**Cloud Pública**: Cifrado de datos en tránsito y en reposo, uso de HSMs y KMS. **Cloud Privada**: Control estricto sobre la localización de datos. **Cloud Híbrida**: Asegurar que los datos críticos permanezcan en la Cloud privada y solo los menos críticos en la pública. **SaaS**: Monitorización y protección de datos sensibles. **IaaS**: Control granular sobre almacenamiento y bases de datos. **PaaS**: Protección en bases de datos gestionadas. **Preferente Migrar:** Para aquellos sistemas con grandes volúmenes de datos sensibles que requieran protección continua. **Cloud First:** Para nuevas aplicaciones que manejen datos personales o confidenciales. **Ubicación de datos críticos**: Considerar Zonas Locales Dedicadas o Regiones Soberanas en proveedores Cloud que cumplan con regulaciones locales y de la EEE, asegurando la ubicación de datos críticos. Cumple con los requisitos de localización de datos y soberanía en infraestructuras, protegiendo

	aislamiento de datos y procesamiento exclusivo. Recomendado por el CCN para garantizar el aislamiento de datos sensibles en entornos críticos. [Guía CCN-STIC-824 Seguridad en Entornos Cloud]	la información en centros regulados en la EEE. [ENS – Cumplimiento Normativo]
3.1.4 Ámbito legal, auditoría y compliance	**Auditoría Continua en Cloud Pública y Multicloud:** Para Cloud Pública y Multicloud, usar herramientas de auditoría continua que generen reportes de cumplimiento en tiempo real y permitan cumplir con los requisitos legales locales e internacionales (RGPD, ENS, ISO 27001). **Auditoría en Cloud Privada:** En Cloud Privada, se deben desarrollar procesos manuales para la auditoría, pero integrando herramientas automáticas en IaaS y PaaS que detecten anomalías en tiempo real. **Monitoreo Intensivo en Aplicaciones Críticas en Cloud Last:** En caso de ser una aplicación crítica bajo un enfoque Cloud Last, el monitoreo debe ser más intensivo para garantizar que se cumplan los requisitos legales.	**Cloud Pública**: Auditoría automatizada en todas las capas de la arquitectura. **Cloud Privada**: Procesos manuales con integración de herramientas automáticas para conformidad y cumplimiento. **Cloud Híbrida**: Auditoría coherente y centralizada para ambos entornos. **SaaS**: Auditoría de conformidad en aplicaciones gestionadas. **IaaS/PaaS**: Auditoría automatizada de configuración, datos y redes. **FaaS/CaaS**: Auditoría sobre los recursos que alojan las funciones y contenedores. **Preferente No Migrar** aplicaciones que ya cumplen con auditorías exhaustivas. **Migrar Todo** cuando se trate de aplicaciones nuevas que deben cumplir regulaciones globales como RGPD o ISO 27001.
3.1.5 Identificación de proveedores	**Evaluación Continua de Proveedores en Multicloud:** Para entornos Multicloud, evaluar continuamente a los proveedores de servicios mediante auditorías de seguridad y certificación.	**Cloud Pública**: Proveedores certificados globalmente. **Cloud Privada**: Proveedores con foco en conformidad local y sectores regulados.

	Evaluación de Proveedores con Government Lens: Utilizar servicios como Government Lens para evaluar proveedores, aplicando recomendaciones específicas para gobiernos, considerando seguridad, compliance y rendimiento. **Certificaciones en Cloud Pública y Privada:** En entornos Cloud Pública y Cloud Privada, se debe asegurar que los proveedores seleccionados cuenten con certificaciones globales como ISO 27001 y estén alineados con los marcos de seguridad locales como el ENS. **Zero Trust en el Acceso de Proveedores:** Implementar el enfoque Zero Trust, auditando el acceso de terceros y proveedores mediante soluciones de control de acceso y autenticación multifactor (MFA) para limitar los privilegios excesivos. **Selección de Proveedores para SaaS:** La selección de proveedores debe centrarse en su capacidad para proteger datos sensibles y cumplir con las regulaciones locales.	**Cloud Híbrida**: Certificación y auditoría de proveedores que operan tanto en la Cloud privada como en la pública. **SaaS**: Selección de proveedores con foco en la seguridad de datos y conformidad. **IaaS/PaaS**: Selección de proveedores con certificaciones globales (ISO 27001, SOC 2). **Preferente Migrar** a la Cloud si los proveedores seleccionados ofrecen un mayor nivel de seguridad y certificaciones.
3.1.6 Continuidad de negocio	**Plan de Recuperación ante Desastres en Cloud Pública y Multicloud:** Desarrollar un Plan de Recuperación ante Desastres (DRP) utilizando soluciones de backup automatizado y replicación geográfica para Cloud Pública y Multicloud. **Backup en Cloud Privada**: En Cloud Privada, se debe asegurar que los respaldos y réplicas estén disponibles en	**Cloud Pública**: Backup automático con replicación geográfica. **Cloud Privada**: Replicación de datos en diferentes ubicaciones controladas. **Cloud Híbrida**: Los datos críticos en Cloud privada y los menos críticos en pública, con soluciones de recuperación automática en ambos.

	diferentes ubicaciones físicas, pero bajo control de la organización. **Recuperación Automática en IaaS y PaaS**: En modelos IaaS y PaaS, asegurar la recuperación automática de las máquinas virtuales, bases de datos y almacenamiento. **Replicación de Datos Críticos en SaaS:** En entornos SaaS, garantizar que los datos críticos de la empresa estén replicados y accesibles en caso de fallas.	**IaaS/PaaS**: Backup y recuperación automática de bases de datos, almacenamiento y cómputo. **SaaS**: Garantizar la disponibilidad continua de los datos alojados en las aplicaciones SaaS. **Cloud First** para nuevas aplicaciones críticas que requieran disponibilidad continua. **Cloud Last** si se prioriza el control de la recuperación en un entorno on-premise.
3.1.7 Training y formación	**Capacitación Continua en Ciberseguridad**: Implementar un programa de capacitación continua en ciberseguridad para los empleados que interactúan con servicios Cloud, alineado con los modelos Zero Trust y Seguridad Basada en el Riesgo. **Formación en Mejores Prácticas de Cloud**: Promover la formación continua en mejores prácticas de Cloud: capacitar a los equipos en el uso de herramientas de monitoreo y seguridad en entornos Cloud. **Entrenamiento en Herramientas de Monitoreo y Seguridad**: Asegurar que los equipos sean competentes en el uso de herramientas para monitoreo, seguridad y resiliencia en entornos Cloud. **Formación en Cloud Pública y Multicloud**: En Cloud Pública y Multicloud, utilizar plataformas de formación como AWS Training and Certification o Microsoft Learn para	**Cloud Pública**: Capacitación sobre las nuevas herramientas de ciberseguridad y riesgos. **Cloud Híbrida**: Formación en la gestión y seguridad de recursos tanto en la Cloud como en entornos on-premise. **Cloud Privada**: Formación sobre gestión local de infraestructuras seguras. **IaaS/PaaS**: Capacitación técnica para la administración segura de la infraestructura. **SaaS**: Formación sobre la gestión de accesos y políticas de cumplimiento. **Cloud First** para formación continua en herramientas de seguridad Cloud. **Limitar Migración** a Cloud si no existe una formación adecuada en el uso seguro de las nuevas tecnologías.

	mantener al personal actualizado sobre los nuevos riesgos y prácticas de seguridad. **Formación en IaaS y PaaS**: En entornos IaaS y PaaS, centrarse en la formación de administradores de infraestructura y redes para gestionar correctamente las configuraciones de seguridad. **Formación en SaaS**: En SaaS, enfocar la formación en la gestión de accesos, control de datos y políticas de cumplimiento.	

3.2 USUARIOS E IDENTIDADES

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones estrategia Cloud
3.2.1 Gobierno de accesos e identidades	**Arquitectura Zero Trust:** Implementar una arquitectura basada en Zero Trust, donde cada solicitud de acceso sea verificada de forma continua. **Control de Acceso Condicional:** Habilitar el control de acceso condicional: Implementar reglas de acceso que restrinjan el acceso según el contexto, como la ubicación geográfica, dispositivo utilizado o riesgos detectados. **Gestión Centralizada de Identidades en Multicloud y Cloud Híbrida:** Para entornos Multicloud y Cloud Híbrida, es importante centralizar la gestión de identidades mediante Identity and Access Management (IAM) para	**Enfoque Zero Trust:** Aplicar el enfoque Zero Trust para limitar estrictamente el acceso de los empleados del CSP a los datos, utilizando autenticación multifactor (MFA) y cifrado. Alineado con el control de acceso y autenticación fuerte del ENS, que requiere el uso de MFA y el cifrado para proteger el acceso a los sistemas. [ENS - Anexo II: Medidas de Seguridad]**.** **Cloud Pública**: IAM centralizado con autenticación MFA. **Cloud Híbrida**: Gestión de identidades federadas entre on-premise y Cloud. **Cloud Privada**: Gestión local con integración IAM.

	asegurar políticas coherentes entre las distintas plataformas y entornos on-premise. **Autenticación Multifactor en IaaS, PaaS y SaaS:** En IaaS, PaaS y SaaS, se debe asegurar que los accesos a las aplicaciones y recursos se realicen bajo autenticación multifactor (MFA) y controles basados en el principio de privilegios mínimos. **Gestión de Accesos en Cloud Privada:** En Cloud Privada, los accesos pueden ser gestionados localmente, pero integrados con soluciones IAM de terceros para habilitar una identidad federada. **Seguridad Basada en el Riesgo:** Analizar los accesos de los usuarios en tiempo real para ajustar los permisos y evitar el acceso indebido.	**IaaS/PaaS**: Gestión granular de identidades para máquinas virtuales, redes y almacenamiento. **SaaS**: Autenticación multifactor y acceso condicional a aplicaciones alojadas en la Cloud. **Cloud First** para nuevas aplicaciones con múltiples usuarios. **Limitar Migración** para sistemas que ya cuentan con IAM robusto on-premise.
3.2.2 Gestión de accesos privilegiados	**Gestión de Accesos Privilegiados:** Implementar soluciones de Privileged Access Management (PAM) para gestionar y auditar los accesos de administradores y usuarios privilegiados. **Políticas de Privilegios Mínimos (PoLP):** Establecer políticas de privilegios mínimos, asignando a cada usuario el nivel mínimo de permisos necesarios para realizar sus tareas, reduciendo el riesgo de comprometer sistemas sensibles. **Automatización de Provisión y Desprovisión de Identidades:** Automatizar la provisión y desprovisión de	**Cloud Pública**: Auditoría continua de accesos privilegiados. **Cloud Privada**: Control estricto de los accesos administrativos locales. **Cloud Híbrida/MultiCloud**: Centralización de la gestión de accesos privilegiados entre entornos. **IaaS/PaaS**: Control granular de accesos de administradores en bases de datos y máquinas virtuales. **SaaS**: Auditoría y control de accesos privilegiados a nivel de aplicación.

	identidades mediante flujos automatizados para la creación y eliminación de usuarios al ingresar o salir de la organización. **Auditoría Continua en Cloud Pública y Multicloud:** En Cloud Pública y Multicloud, auditar continuamente los accesos y restringir los privilegios mediante soluciones IAM y PAM. **Gestión Centralizada de Accesos en Cloud Híbrida:** En Cloud Híbrida, centralizar la gestión de los accesos privilegiados a través de una plataforma común que permita asegurar tanto los entornos Cloud como on-premise. **Restricción de Accesos Privilegiados en SaaS:** En **SaaS**, los accesos privilegiados deben ser restringidos y auditados a nivel de aplicación. **Control de Acceso Granular en IaaS y PaaS:** Para servicios IaaS y PaaS, implementar políticas de control de acceso granular que limiten los privilegios de administrador en máquinas virtuales, bases de datos y almacenamiento.	**Preferente Migrar** aplicaciones críticas que requieren control y auditoría continua de los accesos privilegiados. **Cloud First** para nuevas aplicaciones con múltiples administradores.
3.2.3 Evaluación de patrones de uso	**Monitorización de Recursos en Multicloud y Cloud Pública:** En entornos **Multicloud** y **Cloud Pública**, utilizar servicios nativos de analítica para monitorizar el uso de los recursos y usuarios. **Monitoreo Continuo en IaaS y PaaS:** Para IaaS y PaaS, implementar soluciones de monitoreo continuo que	**Cloud Pública**: Monitoreo continuo del comportamiento del usuario y análisis de patrones. **Cloud Privada**: Evaluación manual con soporte de herramientas de analítica en tiempo real. **Cloud Híbrida/MultiCloud:** Análisis unificado del comportamiento de usuarios en todos los entornos.

	detecten cualquier patrón inusual en el uso de máquinas virtuales, almacenamiento y redes. **Uso de Machine Learning para Detección de Anomalías:** Implementar machine learning para analizar el comportamiento de los usuarios y detectar anomalías en tiempo real.	**IaaS/PaaS**: Monitorización de patrones de uso en máquinas virtuales, almacenamiento y redes. **SaaS**: Detección de comportamientos anómalos en el uso de aplicaciones alojadas en la Cloud. **Preferente Migrar** aquellas aplicaciones donde los patrones de uso pueden implicar riesgos de seguridad. **Cloud First** para aplicaciones nuevas que requieren monitoreo continuo de usuarios y patrones de uso.

3.3 INTEGRACIÓN

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones estrategia Cloud
3.3.1 Interoperabilidad	**Estrategia de Interoperabilidad entre Sistemas On-Premise y Cloud:** Desarrollar una estrategia de interoperabilidad que garantice la integración fluida entre sistemas on-premise y Cloud. **Uso de APIs Abiertas y Protocolos Estándar en Cloud Pública y Multicloud:** En entornos Cloud Pública y Multicloud, es esencial usar APIs abiertas y protocolos estándar como OAuth o SAML para la autenticación y autorización entre sistemas. **Orquestación en IaaS y PaaS:** Para IaaS y PaaS, utilizar plataformas de orquestación como Kubernetes o Anthos	**Cloud Pública**: Uso de APIs abiertas para garantizar la interoperabilidad entre servicios. **Cloud Híbrida**: Uso de tecnologías como Kubernetes o similares para gestionar aplicaciones híbridas. **MultiCloud**: Estrategia de interoperabilidad entre Clouds mediante APIs y herramientas de orquestación. **IaaS/PaaS**: Interoperabilidad de aplicaciones y contenedores entre Clouds y on-premise mediante herramientas como Kubernetes o similares.

	para facilitar la interoperabilidad de aplicaciones y contenedores. **Zonas Locales Dedicadas:** Garantizar que los datos y aplicaciones críticas estén ubicados en centros de datos designados mediante Zonas Locales Dedicadas para cumplir con regulaciones del ENS. Cumple con las directrices del CCN en cuanto a la soberanía de los datos y su ubicación en infraestructuras que garanticen el cumplimiento normativo local. [Guía CCN-STIC-817 Protección de Infraestructuras Críticas]	**SaaS**: Integración fluida mediante APIs y protocolos de autenticación estándar. **Cloud First** para nuevas aplicaciones que requieren interoperabilidad entre Clouds y sistemas legados. **Limitar Migración** si los sistemas actuales ya cuentan con la interoperabilidad necesaria.
3.3.2 Lock-In y portabilidad	**Uso de Contenedores para Evitar Vendor Lock-In:** Para evitar el vendor lock-in, es recomendable utilizar contenedores y tecnologías de orquestación que permitan la portabilidad de aplicaciones entre diferentes proveedores Cloud. **Portabilidad en Cloud Pública y Multicloud:** En Cloud Pública y Multicloud, es esencial diseñar arquitecturas que sean portables, utilizando Kubernetes para facilitar la migración entre Clouds. **Replicabilidad en IaaS** En IaaS, es importante diseñar máquinas virtuales que sean fácilmente replicables en diferentes Clouds.	**Cloud Pública**: Utilizar herramientas que eviten el lock-in, como contenedores y Kubernetes. **Cloud Híbrida/MultiCloud**: Tecnologías de orquestación para asegurar la portabilidad entre diferentes Clouds. **Cloud Privada**: Mantener portabilidad para migraciones futuras a la Cloud pública. **IaaS**: Máquinas virtuales replicables en diferentes Clouds. **PaaS/CaaS**: Orquestación y portabilidad de aplicaciones mediante Kubernetes. **SaaS**: Migración sencilla de aplicaciones a otras Clouds mediante APIs abiertas. **Preferente Migrar** a la Cloud aquellas aplicaciones que puedan beneficiarse de una mayor portabilidad.

		Cloud First para aplicaciones nuevas que puedan ser portadas fácilmente a otras Clouds.
3.3.3 Analíticas de seguridad	**Implementación de Soluciones SIEM:** Implementar soluciones de Security Information and Event Management (SIEM) para correlacionar eventos de seguridad y generar alertas automáticas. **Análisis Centralizado en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, es esencial usar servicios de análisis centralizados para monitorear y gestionar las amenazas de seguridad en tiempo real. **Monitoreo de Infraestructura y Datos en IaaS y PaaS:** Para IaaS y PaaS, las analíticas deben centrarse en el monitoreo de la infraestructura y los datos sensibles alojados.	**Cloud Pública**: Analítica centralizada de eventos de seguridad mediante SIEM. **Cloud Híbrida**: Análisis de seguridad en tiempo real para ambos entornos.plan de **MultiCloud**: Correlación de eventos de seguridad en diferentes plataformas de Cloud. **IaaS/PaaS**: Analítica de seguridad centrada en la infraestructura y los datos sensibles. **SaaS**: Analítica de eventos de seguridad en aplicaciones gestionadas en la Cloud. **Preferente Migrar** aplicaciones críticas que se beneficien de un monitoreo continuo de eventos de seguridad. **Cloud First** para aplicaciones nuevas que requieran analíticas avanzadas de seguridad.
3.3.4 Modelos públicos, privados o híbridos	**Uso de Balanceadores de Carga y CDN para Escalabilidad:** Usar balanceadores de carga y redes de distribución de contenido (CDN) para mejorar la resiliencia y rendimiento, gestionando picos de demanda de manera eficiente. **Definición del Modelo de Despliegue Óptimo:** Definir el modelo de despliegue óptimo para cada aplicación o	**Cloud Pública**: Datos críticos protegidos por cifrado y políticas de acceso restrictivas. **Cloud Privada**: Datos críticos alojados en entornos controlados. **Cloud Híbrida**: Alojamiento de datos críticos en la Cloud privada y procesamiento en la pública.

	servicio, evaluando la sensibilidad de los datos y los requisitos de conformidad. **Protección de Datos Altamente Sensibles en Cloud Privada o Híbrida:** Para datos altamente sensibles, optar por un modelo Cloud Privada o Híbrido donde los datos críticos permanezcan en entornos controlados. En Cloud Pública, asegurar que los datos críticos estén cifrados y protegidos por políticas de acceso restrictivas. **Consistencia de Políticas de Seguridad en Multicloud:** En Multicloud, asegurar la consistencia en las políticas de seguridad entre todas las Clouds públicas y privadas.	**IaaS**: Implementación de políticas de seguridad en la infraestructura y los datos. **PaaS**: Asegurar la conformidad en bases de datos gestionadas. **SaaS**: Protección de datos sensibles en aplicaciones gestionadas en la Cloud. **Cloud First** para aplicaciones nuevas que requieren escalabilidad en la Cloud pública y protección de datos críticos en la Cloud privada. **Cloud Last** si los datos críticos deben permanecer en un entorno on-premise.
3.3.5 Securizar la conexión con sistemas y datos	**Cifrado Extremo a Extremo en Conexiones entre Sistemas On-Premise y Cloud:** Implementar cifrado extremo a extremo en todas las conexiones entre sistemas on-premise y Cloud. **Uso de VPNs y Túneles Cifrados en Cloud Pública y Multicloud:** En Cloud Pública y Multicloud, es recomendable utilizar VPNs y túneles cifrados para proteger el tráfico de red entre los servicios. **Protección de Conexiones en IaaS** Para IaaS, es esencial proteger las conexiones entre las máquinas virtuales y los recursos de almacenamiento mediante firewalls y redes privadas. **Protección del Tráfico en Cloud Privada:** En entornos Cloud Privada, el enfoque debe estar en la protección del	**Cloud Pública:** Cifrado extremo a extremo del tráfico entre sistemas Cloud y on-premise. **Cloud Híbrida:** Protección de las conexiones mediante VPNs y túneles cifrados. **Cloud Privada:** Protección del tráfico dentro de redes internas mediante firewalls y VPNs. **IaaS:** Protección del tráfico entre máquinas virtuales y almacenamiento mediante firewalls y redes privadas. **PaaS/SaaS:** Protección del tráfico de aplicaciones gestionadas mediante cifrado extremo a extremo. **Preferente Migrar** aplicaciones que requieren conexiones seguras y cifradas entre on-premise y la Cloud.

	tráfico dentro de las redes internas mediante VPNs y firewalls. **Implementación de CASB para Control de Acceso en la Cloud**: Usar un broker de seguridad de acceso a la Cloud (CASB) para monitorizar y controlar accesos, asegurando cumplimiento y protección de datos.	**Cloud First** para nuevas aplicaciones que requieren protección en todas las conexiones entre sistemas**.**
3.3.6 Gestión de eventos	**Estrategia de Gestión de Incidentes:** Implementar una estrategia de gestión de incidentes que permita la detección, clasificación y respuesta automática ante incidentes de seguridad. **Automatización de Respuesta en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, utilizar herramientas de orquestación de seguridad como SOAR (Security Orchestration, Automation and Response) para automatizar la respuesta a incidentes. **Gestión de Incidentes en IaaS y PaaS:** En IaaS y PaaS, las soluciones de gestión de incidentes deben enfocarse en el monitoreo y la corrección de problemas en la infraestructura.	**Cloud Pública**: Gestión automatizada de incidentes mediante SOAR. **Cloud Híbrida**: Estrategia de gestión de eventos unificada entre los entornos cloud y on-premise. **Multicloud**: Gestión de incidentes centralizada entre múltiples plataformas cloud. **IaaS/PaaS**: Gestión de incidentes centrada en la infraestructura y los recursos alojados **SaaS**: Gestión de incidentes de seguridad a nivel de aplicación. **Preferente Migrar** a la cloud aquellas aplicaciones que requieren una respuesta automática y eficiente ante incidentes de seguridad. **Cloud First** para nuevas aplicaciones que requieren gestión avanzada de eventos de seguridad.

3.4 SEGURIDAD DE DATOS

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones estrategia Cloud
3.4.1 Clasificación de datos	**Política de Clasificación de Datos:** Implementar una política de clasificación de datos que permita categorizar la información almacenada según su nivel de sensibilidad. **Clasificación Centralizada en Multicloud y Cloud Híbrida:** En entornos Multicloud y Cloud Híbrida, es esencial que la clasificación esté centralizada y sincronizada entre Clouds y sistemas on-premise para evitar la exposición de datos críticos en la Cloud Pública. **Protección de Datos Sensibles en IaaS y PaaS:** En IaaS y PaaS, se debe asegurar que los datos sensibles estén protegidos mediante cifrado y políticas de acceso específicas según la clasificación. **Controles de Acceso en Cloud Privada:** En Cloud Privada, implementar controles de acceso basados en la clasificación de datos para evitar el acceso no autorizado.	**Prohibir la subida de información clasificada de nivel superior a Difusión Limitada a la Cloud Pública.** Se debe usar Cloud Privada o Cloud Híbrida para información clasificada con nivel ALTO en las dimensiones de Confidencialidad (C), Integridad (I), Disponibilidad (A) y Trazabilidad (T).[ENS - Anexo II: Medidas de Seguridad] **Cloud Pública**: Clasificación automática y protección de datos sensibles en tiempo real. **Cloud Híbrida**: Clasificación centralizada de datos entre Clouds y sistemas on-premise. **Cloud Privada**: Control estricto de acceso basado en la clasificación de datos sensibles. **IaaS/PaaS**: Protección de datos clasificados mediante cifrado y control de acceso**.** **SaaS**: Clasificación de datos a nivel de aplicación para asegurar la protección de información confidencial. **Preferente Migrar** aquellos sistemas que se beneficiarán de una mejor protección mediante clasificación automática de datos. **Cloud First** para nuevas aplicaciones que manejan datos sensibles.

3.4.2 Backup y retención de datos	**Estrategia de Backup y Retención de Datos:** Desarrollar una estrategia de backup y retención de datos que garantice que los datos críticos estén respaldados de manera segura y se mantengan según los requisitos de conformidad. **Replicación Geográfica en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, utilizar soluciones de replicación geográfica para asegurar que los datos estén disponibles en caso de fallas regionales. **Backup en Diferentes Ubicaciones Físicas en Cloud Privada:** En Cloud Privada, los backups deben estar replicados en diferentes ubicaciones físicas bajo control directo de la organización. **Backups en IaaS y PaaS:** En IaaS y PaaS, asegurar que los backups incluyan bases de datos, almacenamiento y máquinas virtuales.	**Cloud Pública**: Backup automático con replicación geográfica. **Cloud Híbrida**: Replicación de datos críticos entre Clouds públicas y privadas. **Cloud Privada**: Replicación de datos en ubicaciones controladas por la organización. **IaaS/PaaS**: Backup de máquinas virtuales, bases de datos y almacenamiento con políticas de retención automatizadas. **SaaS**: Asegurar que los datos de aplicaciones gestionadas estén respaldados y disponibles en caso de fallo. **Preferente Migrar** aplicaciones que se beneficiarán de políticas automáticas de backup y recuperación. **Cloud First** para aplicaciones críticas que requieran disponibilidad continua y recuperación rápida en caso de desastre.
3.4.3 Cifrado, tokenización y secretos	**Cifrado Extremo a Extremo:** Implementar cifrado extremo a extremo y control de acceso granular en entornos single-tenant o Cloud Privada para proteger los datos sensibles tanto en tránsito como en reposo. [Guía CCN-STIC-460 Protección ante DDoS](https://www.ccn-cert.cni.es/guias.html). **Gestión Centralizada de Claves en Multicloud y Cloud Híbrida:** En entornos Multicloud y Cloud Híbrida, se debe asegurar que los datos críticos estén cifrados y	**Cloud Pública**: Cifrado extremo a extremo de datos sensibles con gestión de claves centralizada. **Cloud Híbrida**: Gestión unificada de las claves de cifrado entre Clouds y sistemas on-premise. **Cloud Privada**: Protección avanzada de datos mediante cifrado y tokenización. **IaaS/PaaS**: Cifrado de datos sensibles en almacenamiento, bases de datos y máquinas virtuales.

	que las claves de cifrado estén gestionadas centralmente mediante Hardware Security Modules (HSMs) o Key Management Services (KMS). **Tokenización y Control de Acceso en IaaS y PaaS:** En IaaS y PaaS, los datos sensibles deben estar tokenizados y gestionados con políticas estrictas de control de acceso.	**SaaS**: Protección de los datos gestionados por aplicaciones SaaS mediante cifrado y políticas de control de acceso. **Preferente Migrar** aquellas aplicaciones que manejan datos sensibles y se beneficiarían de una gestión centralizada de claves y cifrado. **Cloud First** para nuevas aplicaciones que manejan información confidencial.
3.4.4 Propiedad y segregación de los datos	**Estrategia de Segregación de Datos:** Implementar una estrategia de segregación de datos que garantice que los datos críticos estén completamente aislados de los datos de otras organizaciones o aplicaciones. **Segmentación en Multicloud y Cloud Pública:** En Multicloud y Cloud Pública, debe asegurar que los datos sensibles estén segmentados mediante VPCs (Virtual Private Cloud) o subredes dedicadas. **Segregación de Datos en Cloud Híbrida** En Cloud Híbrida, mantener la segregación entre los datos críticos alojados en la Cloud privada y los datos menos críticos en la Cloud pública. **Políticas de Control de Acceso en IaaS y PaaS:** En IaaS y PaaS, implementar políticas de control de acceso que aseguren que los datos estén segregados según la clasificación.	**Cloud Pública**: Segregación de datos mediante VPCs y subredes dedicadas. **Cloud Híbrida**: Asegurar que los datos críticos estén aislados en la Cloud privada. **Cloud Privada**: Segregación estricta de datos críticos y confidenciales dentro de redes privadas. **IaaS/PaaS**: Implementar VPCs dedicadas y políticas de control de acceso para asegurar la segregación de datos. **SaaS**: Segregación de datos entre diferentes clientes o aplicaciones mediante políticas de acceso. **Cloud First** para aplicaciones nuevas que requieren una segregación avanzada de los datos. **Limitar Migración** si los datos ya están adecuadamente segregados en entornos on-premise. **Infraestructuras multi-tenant:** Prohibir infraestructuras multi-tenant para datos clasificados, optando por entornos single-tenant

		o Clouds privadas dedicadas. Esto se alinea con las guías del CCN, que recomiendan el aislamiento de datos sensibles en entornos dedicados para evitar el acceso no autorizado en entornos compartidos. [Guía CCN-STIC-824 Seguridad en Entornos Cloud]
3.4.5 Evaluación de riesgos	**Estrategia de Evaluación Continua de Riesgos:** Implementar una estrategia de evaluación continua de riesgos para identificar vulnerabilidades en los sistemas y datos alojados en la Cloud. **Análisis de Seguridad en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, utilizar herramientas de análisis de seguridad que evalúen el nivel de riesgo de los datos sensibles y ajusten automáticamente las políticas de protección. **Evaluación de Riesgos en Cloud Privada:** En Cloud Privada, la evaluación de riesgos debe centrarse en la infraestructura interna y su exposición a posibles amenazas externas. **Evaluación de Configuraciones en IaaS y PaaS:** En IaaS y PaaS, las evaluaciones de riesgo deben incluir el análisis de configuraciones, redes y bases de datos.	**Cloud Pública**: Evaluación automática de riesgos en tiempo real para ajustar las políticas de seguridad. **Cloud Híbrida**: Evaluación continua de riesgos tanto en la Cloud pública como en los sistemas on-premise. **Cloud Privada**: Evaluación de riesgos centrada en la infraestructura interna. **IaaS/PaaS**: Evaluación continua de configuraciones, redes y bases de datos para identificar vulnerabilidades. **SaaS**: Evaluación de riesgos en aplicaciones gestionadas para ajustar automáticamente las políticas de seguridad. **Preferente Migrar** aquellas aplicaciones que se beneficiarán de una evaluación continua de riesgos y ajustes automáticos de políticas. **Cloud First** para aplicaciones nuevas que requieren una evaluación avanzada de riesgos.
3.4.6 Data loss	**Implementación de Soluciones de Data Loss Prevention (DLP):** Implementar una solución de Data	**Cloud Pública**: DLP automatizado para monitorear y bloquear la fuga de datos sensibles.

prevention (DLP)	Loss Prevention (DLP) para evitar la fuga de datos sensibles. **Monitoreo y Protección en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, utilizar DLP para monitorear el acceso y la transferencia de datos entre los servicios Cloud y los usuarios. **Protección de Datos en Cloud Privada** En Cloud Privada, enfocar la protección en los datos sensibles dentro de las redes internas y asegurarse de que no se filtren a sistemas externos. **Políticas de DLP en IaaS y PaaS:** En IaaS y PaaS, implementar políticas de DLP que monitoreen y bloqueen cualquier intento de transferir datos sensibles sin autorización.	**Cloud Híbrida**: Implementar DLP tanto en los entornos Cloud como on-premise para asegurar que los datos sensibles estén protegidos en todos los puntos. **Cloud Privada**: Protección de datos internos mediante DLP. **IaaS/PaaS**: Implementación de políticas de DLP que monitoreen y bloqueen intentos de fuga de datos. **SaaS**: Protección de datos sensibles en aplicaciones gestionadas mediante DLP y políticas de control de acceso. **Preferente Migrar** a la Cloud aquellas aplicaciones que manejan grandes volúmenes de datos sensibles y que se beneficiarían de soluciones automáticas de DLP. **Cloud First** para nuevas aplicaciones que manejan datos confidenciales.
3.4.7 Almacenamiento y eliminación segura	**Políticas de Almacenamiento Seguro y Eliminación Definitiva de Datos:** Implementar políticas de almacenamiento seguro y eliminación definitiva de datos conforme a las normativas locales e internacionales. **Cifrado y Eliminación Irreversible en Multicloud y Cloud Pública:** En entornos Multicloud y Cloud Pública, debe asegurar que los datos sensibles estén cifrados y que los datos eliminados sean destruidos de manera irreversible. **Eliminación Segura en Cloud Privada:** En Cloud Privada, gestionar los datos bajo estrictas políticas de	**Cloud Pública**: Implementar políticas de eliminación irreversible de datos tras su ciclo de vida. **Cloud Híbrida**: Asegurar que tanto en la Cloud como en los sistemas on-premise, los datos se eliminen de forma segura y permanente. **Cloud Privada**: Estrictas políticas de almacenamiento y eliminación segura de datos. **IaaS/PaaS**: Implementación de herramientas de eliminación segura en máquinas virtuales, almacenamiento y bases de datos.

	eliminación segura que garanticen que no queden rastros de la información después de su eliminación. **Eliminación Segura en IaaS y PaaS:** En IaaS y PaaS, implementar herramientas que garanticen la eliminación segura de datos en máquinas virtuales, almacenamiento y bases de datos.	**SaaS**: Asegurar que los datos almacenados por aplicaciones gestionadas sean eliminados de manera irreversible al finalizar su ciclo de vida. **Cloud First** para nuevas aplicaciones que requieren almacenamiento seguro y políticas de eliminación de datos según normativas locales. **Preferente No Migrar** si los datos ya se gestionan bajo políticas adecuadas de eliminación en on-premise.
3.4.8 Auditoría de datos y análisis forense	**Sistema de Auditoría Continua:** Implementar un sistema de auditoría continua que registre todos los accesos y modificaciones de datos, generando alertas automáticas ante actividades sospechosas. **Auditoría Centralizada en Multicloud y Cloud Pública:** En Multicloud y Cloud Pública, utilizar herramientas de auditoría centralizada que correlacionen eventos de seguridad y permitan el análisis forense en caso de incidentes. **Auditoría Focalizada en Cloud Privada:** En Cloud Privada, la auditoría debe centrarse en los accesos a los datos críticos y asegurar que cualquier modificación esté registrada y disponible para análisis posterior. **Auditoría en IaaS y PaaS:** En IaaS y PaaS, la auditoría debe incluir configuraciones, redes, almacenamiento y bases de datos.	**Cloud Pública**: Auditoría centralizada y automatizada de accesos y modificaciones de datos. **Cloud Híbrida**: Asegurar que tanto en los entornos Cloud como on-premise se registren y auditen todas las actividades relacionadas con los datos. **Cloud Privada**: Auditoría continua de accesos y modificaciones de datos críticos. **IaaS/PaaS**: Auditoría de configuraciones, redes, almacenamiento y bases de datos. **SaaS**: Auditoría de accesos y modificaciones en aplicaciones gestionadas, con capacidad de análisis forense en caso de incidentes. **Preferente Migrar** aplicaciones que requieren una auditoría avanzada y continua de datos y accesos.

		Cloud First para nuevas aplicaciones críticas que requieren un monitoreo y auditoría exhaustiva de los datos y accesos.

3.5 PLATAFORMAS Y APLICACIONES

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones estrategia Cloud
3.5.1 Identificación de vulnerabilidades y amenazas en SDLC, DevOps y actualización de aplicaciones	**Automatizar pruebas de seguridad en el pipeline de CI/CD:** Incluir pruebas automáticas de seguridad durante el desarrollo de aplicaciones en las fases de integración y despliegue continuo (CI/CD)**.** **Estrategia de Seguridad en el Ciclo de Vida del Desarrollo de Software (SDLC):** Implementar una estrategia de seguridad en el ciclo de vida del desarrollo de software (SDLC) que asegure que las aplicaciones y actualizaciones pasen por fases de análisis de vulnerabilidades y pruebas de seguridad. **Automatización de Identificación de Amenazas en Multicloud y Cloud Pública:** En Multicloud y Cloud Pública, utilizar herramientas nativas que automaticen la identificación de amenazas y vulnerabilidades en cada fase del desarrollo. **Integración de DevSecOps en IaaS y PaaS**: En entornos IaaS y PaaS, integrar DevSecOps para garantizar que la seguridad esté incorporada en cada	**Cloud Pública**: Integración de herramientas nativas para análisis automático de vulnerabilidades. **Cloud Híbrida**: Seguridad integrada en el ciclo de vida del desarrollo tanto en la Cloud como en on-premise. **Cloud Privada**: Probar vulnerabilidades en fases previas antes de la implementación en producción. **IaaS/PaaS**: DevSecOps integrado en el ciclo de vida del desarrollo para asegurar aplicaciones y configuraciones antes del despliegue. **SaaS**: Asegurar que las aplicaciones gestionadas pasen por análisis de seguridad antes de ser actualizadas. **Preferente Migrar** aquellas aplicaciones que se beneficiarían de un ciclo de desarrollo seguro y automatizado. **Cloud First** para nuevas aplicaciones que requieran una integración continua y seguridad desde la fase de desarrollo.

	fase de la implementación, desde el código hasta el despliegue en producción.	
3.5.2 Control de acceso a nivel de aplicaciones	**Controles de Acceso Granular a Nivel de Aplicaciones:** Implementar controles de acceso granular a nivel de aplicaciones, asegurando que los usuarios solo puedan acceder a las funciones y datos necesarios según su rol. **Gestión de Accesos en Cloud Pública y Multicloud:** En entornos Cloud Pública y Multicloud, utilizar servicios de IAM para gestionar el acceso de los usuarios a los recursos y aplicaciones en función de políticas centralizadas. **Autenticación Multifactor en IaaS y PaaS:** En IaaS y PaaS, gestionar el acceso a las aplicaciones mediante soluciones de autenticación multifactor (MFA) y políticas de acceso condicional basadas en roles.	**Cloud Pública**: Gestión de acceso mediante IAM centralizado y autenticación MFA. **Cloud Híbrida**: Políticas de acceso coherentes entre los entornos Cloud y on-premise. **Cloud Privada**: Control estricto del acceso a las aplicaciones y datos sensibles. **IaaS/PaaS**: Implementación de políticas de acceso condicional y MFA para proteger las aplicaciones en la infraestructura y plataformas. **SaaS**: Asegurar el control de acceso granular a las funciones y datos en aplicaciones gestionadas. **Preferente Migrar** a la Cloud aquellas aplicaciones que requieren un control avanzado de accesos a nivel de aplicación. **Cloud First** para nuevas aplicaciones con múltiples usuarios y roles diferenciados.
3.5.3 Gestión / Monitorización	**Monitoreo continuo de la seguridad de aplicaciones:** Implementar herramientas de monitoreo que analicen continuamente el estado de seguridad de las aplicaciones, generen alertas ante posibles vulnerabilidades o anomalías, y permitan una respuesta rápida ante incidentes.	**Cloud Pública**: Monitorización centralizada de todas las aplicaciones mediante herramientas nativas. **Cloud Híbrida**: Monitoreo coherente entre los entornos on-premise y la Cloud.

	Implementar un sistema de respuesta automática a incidentes: Integrar herramientas de respuesta a incidentes que activen acciones automáticas ante alertas de seguridad, reduciendo el tiempo de reacción ante posibles amenazas. **Estrategia de Monitorización Continua:** Implementar una estrategia de **monitorización continua** que permita gestionar el rendimiento, la seguridad y la disponibilidad de las aplicaciones en tiempo real. **Centralización del Monitoreo en Cloud Pública y Multicloud:** En **Cloud Pública** y **MultiCloud**, utilizar servicios nativos que permitan centralizar el monitoreo de todas las aplicaciones y recursos desde un solo panel. **Monitorización en Tiempo Real en IaaS y PaaS:** En entornos **IaaS** y **PaaS**, es importante asegurar que las aplicaciones críticas estén monitorizadas mediante alertas y métricas en tiempo real para detectar problemas de rendimiento o seguridad.	**Cloud Privada**: Monitorización continua de aplicaciones críticas y sensibles dentro de la infraestructura privada. **IaaS/PaaS**: Monitoreo continuo de las aplicaciones en la infraestructura y plataformas para asegurar su rendimiento y seguridad. **SaaS**: Monitoreo del uso, disponibilidad y rendimiento de las aplicaciones gestionadas en la Cloud. **Preferente Migrar** a la Cloud aquellas aplicaciones críticas que requieren un monitoreo continuo de su rendimiento y seguridad. **Cloud First** para nuevas aplicaciones que se beneficiarán de una monitorización centralizada y automatizada.
3.5.4 Gestión de vulnerabilidades de aplicaciones y búsqueda de solución	**Automatizar la gestión de parches:** Implementar un sistema automatizado para la aplicación de parches y actualizaciones de seguridad en las aplicaciones, reduciendo el riesgo de exposición a vulnerabilidades críticas.	**Cloud Pública**: Gestión automática de vulnerabilidades con alertas y parches en tiempo real. **Cloud Híbrida**: Asegurar que tanto las aplicaciones en la Cloud como on-premise sean monitorizadas y protegidas frente a vulnerabilidades.

	Implementar soluciones de protección contra pérdida de datos (DLP): Usar herramientas que detecten y eviten la exfiltración de datos sensibles, asegurando que la información crítica no sea compartida de manera no autorizada o expuesta a riesgos de seguridad. **Sistema de Gestión de Vulnerabilidades**: Implementar un sistema de gestión de vulnerabilidades que permita identificar, priorizar y corregir cualquier falla de seguridad en las aplicaciones. **Escaneos Automáticos de Vulnerabilidades en Cloud Pública y Multicloud**: En entornos Cloud Pública y MultiCloud, utilizar soluciones nativas para realizar escaneos automáticos de vulnerabilidades y generar alertas en tiempo real. En IaaS y PaaS, es esencial integrar estos servicios en las fases de desarrollo y despliegue para asegurar que las aplicaciones estén protegidas desde el principio. **Integración de Gestión de Vulnerabilidades en IaaS y PaaS:** En IaaS y PaaS, integrar estos servicios en las fases de desarrollo y despliegue para asegurar que las aplicaciones estén protegidas desde el principio.	**Cloud Privada**: Identificación manual y corrección de vulnerabilidades. **IaaS/PaaS**: Escaneo automático de vulnerabilidades en la infraestructura y plataformas, con generación de alertas y parches. **SaaS**: Asegurar que las aplicaciones gestionadas cuenten con mecanismos de gestión proactiva de vulnerabilidades y correcciones automáticas. **Preferente Migrar** aquellas aplicaciones que se beneficiarían de un monitoreo continuo y una gestión automática de vulnerabilidades. **Cloud First** para nuevas aplicaciones que requieran una corrección proactiva de vulnerabilidades en tiempo real.

3.6 INFRAESTRUCTURA CLOUD

Sección	Recomendaciones Arquitectura Cloud	Recomendaciones estrategia Cloud
3.6.1 Funcionalidad de seguridad	**Integración de Funcionalidades de Seguridad en la Infraestructura Cloud:** Integrar funcionalidades de seguridad en toda la infraestructura Cloud, asegurando que cada recurso tenga controles de seguridad integrados y auditables. En entornos Cloud Pública y Multicloud, implementar soluciones nativas que permitan configurar y monitorear las políticas de seguridad en todos los servicios. **Firewalls Administrados para Protección de Cargas de Trabajo:** Utilizar firewalls administrados para proteger las cargas de trabajo y controlar el tráfico de red, aplicando políticas de seguridad coherentes en entornos Cloud. **Enfoque Zero Trust en la Seguridad de la Infraestructura:** Aplicar políticas de Zero Trust, donde todo acceso a la red o aplicaciones se autentique y autorice continuamente, asegurando que sólo usuarios o servicios validados puedan acceder a los recursos. **Controles de Seguridad en IaaS y PaaS:** En IaaS y PaaS, es esencial asegurar que los controles de seguridad estén presentes en cada nivel de la infraestructura: redes, almacenamiento y cómputo.	**Cloud Pública:** Funcionalidades de seguridad integradas y auditables en toda la infraestructura. **Cloud Híbrida**: Controles de seguridad coherentes en ambos entornos. **Cloud Privada**: Implementar políticas de seguridad avanzadas en redes, almacenamiento y cómputo. **IaaS/PaaS:** Controles de seguridad integrados en redes, almacenamiento y cómputo, con auditoría continua. **SaaS**: Asegurar que las aplicaciones gestionadas tengan controles de seguridad avanzados e integrados en cada capa. **Preferente Migrar** aquellas aplicaciones que requieren funcionalidades de seguridad avanzadas y auditables en tiempo real. **Cloud First** para nuevas aplicaciones críticas que requieran seguridad avanzada integrada en toda la infraestructura.

	Estos controles deben ser consistentes y auditables en todos los servicios y componentes. **Centralización de la Gestión de Seguridad:** En un despliegue Cloud First, utilizar soluciones como AWS Security Hub o Azure Security Center para centralizar la gestión de seguridad de la infraestructura y monitorear en tiempo real cualquier cambio o amenaza, garantizando que las políticas de seguridad se apliquen de forma continua y coherente.	
3.6.2 Gestión de incidentes y gestión de cambios	**Plan de Gestión de Incidentes y Disponibilidad:** Desarrollar un plan de gestión de incidentes que permita responder rápidamente a cualquier problema sin afectar la disponibilidad y seguridad de los servicios. Este plan debe estar alineado con los requisitos de seguridad y continuidad operativa de la organización. **Automatización de la Respuesta a Incidentes con SOAR:** En entornos Cloud Pública y Multicloud, es recomendable utilizar herramientas de SOAR (Security Orchestration, Automation and Response) para automatizar la respuesta a incidentes, permitiendo la aplicación inmediata de medidas correctivas y minimizando el impacto en la operación. **Gestión de Cambios Automatizada y Controlada:** Implementar un sistema de gestión de cambios automatizado que realice un seguimiento continuo de las modificaciones en la infraestructura. Este sistema debe	**Cloud Pública:** Gestión automatizada de incidentes mediante SOAR y auditoría continua. **Cloud Híbrida:** Gestión de incidentes coherente entre ambos entornos. **Cloud Privada:** Control estricto de cambios y respuesta a incidentes críticos dentro de la infraestructura privada. **IaaS/PaaS**: Gestión de incidentes centrada en la infraestructura y plataformas, con respuesta automática ante incidentes críticos. **SaaS**: Gestión de incidentes de seguridad a nivel de aplicación, con capacidad de respuesta automatizada. **Preferente Migrar** aplicaciones que requieren una respuesta rápida y eficiente ante incidentes de seguridad. **Cloud First** para nuevas aplicaciones críticas que requieren una gestión avanzada de cambios e incidentes.

	contar con flujos de trabajo aprobados que evalúen el impacto de los cambios en la configuración y aseguren que cualquier ajuste sea seguro y auditado. **Control de Cambios en IaaS y PaaS:** En IaaS y PaaS, asegurar que la gestión de cambios se realice de manera controlada para evitar interrupciones o fallas en los servicios. Es fundamental que estos cambios sean aprobados y evaluados adecuadamente antes de implementarse. **Centralización de la Gestión de Incidentes en Cloud First:** En un despliegue Cloud First, se recomienda utilizar herramientas como AWS CloudTrail o Azure Monitor para gestionar automáticamente los incidentes y cambios, garantizando que cualquier modificación en los recursos sea segura y esté debidamente auditada.	
3.6.3 Configuración de redes	**Configuración de Redes Seguras:** Implementar una configuración de redes seguras que asegure que el tráfico entre los recursos esté debidamente protegido, garantizando la seguridad y disponibilidad de los datos y aplicaciones. **Implementación de Redes Virtuales Aisladas:** Configurar redes virtuales aisladas que incluyan mecanismos de seguridad avanzados, como VPNs o conexiones privadas, para la interconexión segura de	**Cloud Pública**: Configuración segura de redes mediante VPCs y firewalls. **Cloud Híbrida**: Segmentación de redes entre los recursos Cloud y on-premise para asegurar el tráfico. **Cloud Privada**: Protección avanzada del tráfico entre los recursos mediante redes privadas virtuales y firewalls. **IaaS/PaaS**: Segmentación de redes y protección del tráfico mediante firewalls y redes privadas.

	servicios. Esto permite mantener la privacidad del tráfico en entornos distribuidos y proteger los recursos críticos **Uso de Balanceadores de Carga y CDN Seguros:** Implementar balanceadores de carga y redes de distribución de contenido (CDN) para garantizar alta disponibilidad y rendimiento, asegurando que tanto las conexiones entrantes como salientes estén protegidas. **Protección del Tráfico de Red en Cloud Pública y Multicloud:** En entornos Cloud Pública y Multicloud, es fundamental utilizar VPCs (Virtual Private Clouds) y firewalls para proteger el tráfico de red y garantizar que solo los recursos autorizados puedan intercambiar datos de manera segura. **Segmentación de Redes en IaaS:** En IaaS, es recomendable segmentar las redes para asegurar que solo los usuarios y servicios autorizados puedan acceder a los recursos críticos, limitando el acceso y minimizando el riesgo de exposición de datos sensibles.	**SaaS**: Protección del tráfico de datos entre aplicaciones mediante segmentación de red y firewalls. **Preferente Migrar** a la Cloud aquellas aplicaciones que se beneficiarían de una configuración de redes segura y segmentada. **Cloud First** para nuevas aplicaciones críticas que requieren una configuración avanzada de redes.
3.6.4 Fortalecimiento de la Cloud	**Medidas de Hardening para Fortalecer la Seguridad de la Infraestructura Cloud:** Implementar medidas de hardening para fortalecer la seguridad de la infraestructura Cloud, asegurando que todas las configuraciones estén alineadas con las mejores prácticas de seguridad y protejan los recursos críticos.	**Cloud Pública**: Políticas avanzadas de hardening para proteger la infraestructura contra ataques externos. **Cloud Híbrida**: Fortalecimiento de la infraestructura tanto en la Cloud como en on-premise para asegurar la resiliencia. **Cloud Privada**: Aplicación de hardening a los recursos críticos internos.

	Protección contra Ataques Externos en Cloud Pública y Multicloud: En entornos Cloud Pública y Multicloud, es esencial aplicar políticas de seguridad que protejan contra ataques externos, como DDoS, y aseguren la resiliencia de la infraestructura. **Prohibir el acceso directo desde internet a la infraestructura crítica de la entidad.** [Guía CCN-STIC-460 Protección ante DDoS] **Revisiones Periódicas de la Configuración de Seguridad:** Realizar revisiones automáticas y manuales de la configuración de la infraestructura Cloud para asegurar que se ajusta a las mejores prácticas de seguridad. Estas revisiones deben incluir la verificación de los controles de seguridad aplicados a todos los recursos. **Cifrado de Datos en Reposo y en Tránsito:** Implementar mecanismos de cifrado tanto para los datos en reposo como en tránsito en toda la infraestructura, para proteger la confidencialidad de la información y asegurar que los datos estén protegidos frente a amenazas internas y externas. **Hardening de Máquinas Virtuales en IaaS:** En IaaS, aplicar políticas de hardening a las máquinas virtuales y recursos críticos para evitar vulnerabilidades. Esto incluye asegurar que las configuraciones de seguridad estén optimizadas y que se implementen controles	**IaaS/PaaS:** Hardening de máquinas virtuales y recursos críticos, con políticas de protección avanzadas contra ataques externos. **SaaS:** Protección de las aplicaciones gestionadas mediante políticas avanzadas de seguridad y resiliencia frente a ataques. **Preferente Migrar** aplicaciones que requieren una infraestructura más segura y resiliente frente a ataques externos. **Cloud First** para nuevas aplicaciones críticas que necesitan protección avanzada contra ataques DDoS y vulnerabilidades.

	robustos para proteger los sistemas contra posibles ataques. **Prohibir infraestructuras multi-tenant:** Prohibir infraestructuras multi-tenant para los recursos críticos y asegurar el uso de entornos single-tenant o Clouds privadas para la entidad. [Guía CCN-STIC-824 Seguridad en Entornos Cloud]	
3.6.5 Gestión de vulnerabilidades	**Análisis Automatizados de Vulnerabilidades**: Implementar sistemas de escaneo que identifiquen vulnerabilidades de seguridad en la infraestructura de manera continua y proporcionen recomendaciones para mitigarlas. **Políticas de Actualización de Seguridad Automáticas:** Configurar la infraestructura para aplicar parches de seguridad y actualizaciones de software automáticamente, minimizando el tiempo de exposición a vulnerabilidades. **Estrategia de Gestión Continua de Vulnerabilidades:** Estrategia que permita identificar, priorizar y corregir fallos de seguridad en toda la infraestructura Cloud. **Uso de Herramientas Nativas para la Gestión de Vulnerabilidades**: En entornos Cloud Pública y MultiCloud, utilizar herramientas nativas que automaticen la identificación y corrección de vulnerabilidades en tiempo real.	**Cloud Pública**: Gestión automatizada de vulnerabilidades con correcciones en tiempo real. **Cloud Híbrida**: Gestión coherente de vulnerabilidades tanto en la Cloud como en on-premise. **Cloud Privada**: Identificación y corrección manual de vulnerabilidades en la infraestructura interna. **IaaS/PaaS**: Identificación y corrección automática de vulnerabilidades en la infraestructura y plataformas. **SaaS:** Asegurar que las aplicaciones gestionadas cuenten con mecanismos de corrección automática de vulnerabilidades. **Preferente Migrar** aplicaciones que requieren una corrección automática y continua de vulnerabilidades en tiempo real. **Cloud First** para nuevas aplicaciones que se beneficiarían de un monitoreo continuo y corrección de vulnerabilidades.

	Herramientas Nativas en IaaS y **PaaS;** Es importante integrar estas herramientas en los servicios y recursos para asegurar que cualquier vulnerabilidad sea corregida antes de ser explotada.	
3.6.6 Operaciones de infraestructura	**Monitorización del Uso de Recursos y Optimización del Rendimiento:** Implementar herramientas de monitoreo que permitan visualizar el uso de recursos, optimizar el rendimiento y detectar posibles cuellos de botella. **Sistema de Respaldo Automatizado:** Configurar copias de seguridad automáticas de las instancias y volúmenes de almacenamiento para garantizar la disponibilidad de los datos y la recuperación rápida ante fallos. **Gestión Eficiente y Segura de las Operaciones:** Asegurar que las operaciones de infraestructura Cloud se gestionen de manera eficiente y segura, optimizando el uso de los recursos. **Uso de Herramientas de Gestión Automatizada**: En Cloud Pública y MultiCloud, es recomendable usar herramientas de gestión automatizada que permitan escalar los recursos y monitorizar el rendimiento en tiempo real. **Alineación de las Operaciones con las Políticas de Seguridad**: En IaaS, es importante asegurar que las	**Cloud Pública**: Gestión automatizada de las operaciones, con escalabilidad y optimización continua. **Cloud Híbrida**: Gestión coherente de las operaciones entre los recursos on-premise y Cloud. **Cloud Privada**: Gestión manual de las operaciones internas con optimización continua de recursos. **IaaS/PaaS**: Automatización de las operaciones en la infraestructura y plataformas, con escalabilidad y optimización de los recursos en tiempo real. **SaaS**: Asegurar que las operaciones de las aplicaciones gestionadas sean eficientes y seguras, con monitoreo continuo. **Preferente Migrar** aquellas aplicaciones críticas que se beneficiarán de una gestión automatizada y optimizada de las operaciones. **Cloud First** para nuevas aplicaciones que requieren una gestión eficiente de la infraestructura y sus operaciones.

	operaciones estén alineadas con las políticas de seguridad para evitar comprometer los datos y aplicaciones alojadas.	