Aclaración de las prácticas de privacidad, protección de datos y ciberseguridad de Skyone

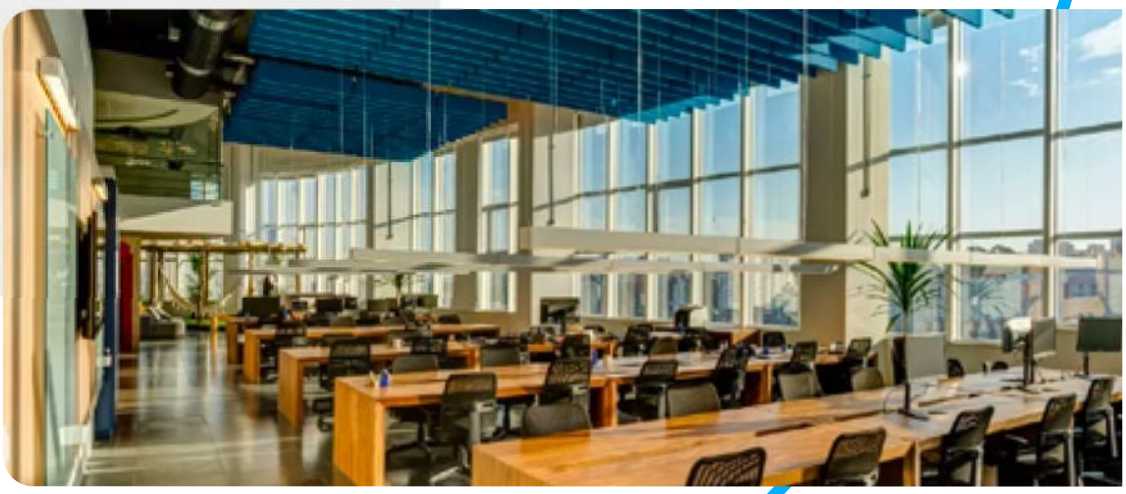
V 1.2

INTRODUCCIÓN

Skyone se dedica a proporcionar servicios de Licencias de Uso de la Plataforma Skyone Autosky y a configurar los entornos indicados en la contratación de los servicios por parte del Cliente final. En este proceso, involucramos nuestras áreas de Gobierno y Operaciones para detectar, resolver, prevenir y reducir incidencias de privacidad, protección de datos y ciberseguridad, proporcionando entornos informáticos cada vez más fiables, disponibles y saludables.
A continuación, enumeramos las respuestas a las preguntas que nos han enviado en varias RFP y auditorías para aclarar cómo actuamos en privacidad, protección de datos y ciberseguridad.

IMPORTANTE:

Si la información de este documento no aclara sus dudas, envíe sus consultas o solicite la programación de una llamada enviando un correo electrónico con sus datos a **governanca@skyone.solutions**



ACERCA DE GOBERNANZA Y OPERACIONES

1. ¿Cuáles son los procesos y procedimientos de privacidad, protección de datos y ciberseguridad que Skyone tiene implementados?

Los procesos y procedimientos son elementos fundamentales y críticos, y en Skyone estamos trabajando para adaptarlos para obtener la certificación de la Norma Técnica ABNT NBR ISO/IEC 27001:2013, la cual especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información.
Hemos implementado los siguientes procesos y procedimientos:

Rutina de análisis de seguridad

Semana tras semana se realizan procesos para identificar y mitigar riesgos en el sistema operativo, interfaces web y bases de datos de la plataforma Skyone Autosky. Esto incluye, pero no se limita a:

- Escaneo de vulnerabilidades superficiales externas e internas;
- Escaneo de la web oscura;
- Aplicación de parches de software;
- Actualizaciones de la versión del sistema operativo;
- Actualizaciones de la versión de la base de datos;
- Escaneo y mapeo de puertas

Plan de gestión de vulnerabilidades

Realizamos el mapeo y clasificación de vulnerabilidades según el Common Vulnerability Scoring System V3.0 (CVSS v3.0 Rating), un marco abierto para comunicar las características y la gravedad de las vulnerabilidades del software. Las clasificamos según:

- Crítico;
- Alto;
- Promedio;
- Bajo

Los procesos regulares aplican las correcciones apropiadas de acuerdo con cada nivel de gravedad y se evidencian en nuestro proceso de Gobernanza de la seguridad.

ACERCA DE GOBERNANZA Y OPERACIONES

Monitoreo, detección y respuesta de rutina

Monitoreo, detección y respuesta de rutina. Realizamos rutinas de análisis y gestión asociadas a nuestro SOC para el seguimiento y alerta de eventos de seguridad mediante tecnología XDR (Extended Detection and Response). Plan de gestión de incidentes de privacidad, protección de datos y ciberseguridad. El plan define de manera sistemática el proceso de atención de eventos e incidentes, llevado a cabo por el área de Gobernanza de Skyone, dentro de su programa de privacidad, protección de datos y ciberseguridad.

Para obtener más información sobre el Plan de Gestión de Incidentes de Privacidad, Protección de Datos y Ciberseguridad, puede solicitar el documento: Plan de Gestión de Incidentes de Privacidad, Protección de Datos y Ciberseguridad. V.1.2 - 25 de octubre de 2022.

Plan de comunicación de incidentes

Hemos implementado un plan de respuesta a incidentes en el que las comunicaciones y la divulgación juegan un papel particularmente importante para la audiencia adecuada: compartir información, construir relaciones y fomentar la confianza. Es importante considerar la comunicación como una iniciativa estratégica. Las comunicaciones trascienden todos los procesos comerciales y de seguridad, tanto los que ocurren en las operaciones normales como durante una crisis.

Para obtener más información sobre el Plan de Comunicación de Incidentes, puede solicitar el documento: Plan de Comunicación de Incidentes - V.1.2 - 18 de agosto de 2022.

Seguridad del dispositivo Skyone

Todos los puntos finales son propiedad de Skyone, con EDR (Endpoint Detection and Response) instalado y supervisado por el equipo de Gobernanza de la seguridad. Los empleados tienen prohibido el uso de equipos personales para actividades y acceso a la empresa, incluso en la condición de trabajo remoto y limitado por el control de herramientas internas y el acceso a través de firewall de borde al sistema interno y al entorno del cliente.

Las puertas USB están bloqueadas para el acceso a la memoria USB.

ACERCA DE GOBERNANZA Y OPERACIONES

Acciones de adaptación, mitigación y seguimiento a riesgos vinculados a la LGPD (Ley General de Protección de Datos de Brasil) y uso de datos de terceros

Disponemos de acciones estructuradas para la adaptación y mitigación de los riesgos vinculados a la LGPD en 2020. Skyone solo recopila datos digitalmente de dos maneras:

- A través de formularios en nuestro sitio web y hotsitesitio de campaña;
- A través de formularios integrados con la herramienta de empresas de marketing

Hemos adoptado las siguientes pautas para garantizar el cumplimiento de la política de privacidad:

- Al enviar cualquier comunicación, ya sea de marketing o relacional, a los contactos de nuestra base de CRM, se genera una solicitud de consentimiento.
- Toda recopilación realizada a través de formularios en el sitio web o hotsites, se informa sobre la política de privacidad, el control de cookies y se solicita el consentimiento.
- El área de Gobernanza es responsable de auditar sistemáticamente si se están siguiendo estos procedimientos.
- No se realizan cambios sin la aprobación del Comité de Privacidad y Protección de Datos.
- Todos los contratos con proveedores fueron auditados y evaluados para incluir cláusulas de privacidad.

2. ¿Cómo es el proceso de reporte de incidentes?

Seguimos pasos estructurados para gestionar un incidente y creamos un portal de registro de incidentes donde cada paso del proceso tiene un propósito claramente definido. La siguiente imagen muestra las actividades macro.

Para un conocimiento más profundo del Plan de Gestión de Incidencias de Privacidad, Protección de Datos y Ciberseguridad, puede solicitar el documento: Plan de Gestión de Incidencias de Privacidad, Protección de Datos y Ciberseguridad. V.1.2 - 25 de octubre de 2022.

3. Procedimiento de Gestión de Cambios (GMUD)

Los cambios en los entornos de nuestros clientes se gestionan dentro de nuestro proceso de Gestión de cambios, que comienza con la identificación del cambio, las fechas, los sistemas afectados, las responsabilidades, los impactos, los planes de prueba previos al cambio, el plan de reversión y el plan de prueba posterior al cambio.

El GMUD se solicita a través del Portal de Clientes vía ticket y luego de ser analizado y aprobado se procede a ejecutar el cambio programado.

4. ¿Cómo funciona el plan de transición en caso de cancelación de contrato Skyone?

En los casos de rescisión unilateral antes del término final del contrato, la necesidad de cumplir con la multa se calculará proporcionalmente a los meses restantes.

Cualquiera que sea la forma de terminación, Skyone se compromete a tener disponible el respaldo de la base de datos por 15 (quince) días a partir de la terminación.

Cualquier solicitud de cancelación se puede solicitar por correo electrónico: cancelamento **cancellation@skyone.solutions.**

5. ¿Cuáles son los SLA para la Política de Backup?

https://skyinone.atlassian.net/wiki/spaces/AUTODOC/pages/136544308/Snapshots+Backups

6. ¿Skyone cuenta con un Código de Ética, Conducta y Política de Gestión de Privacidad?

Sí, nuestro código de ética y política de privacidad es público y se puede acceder a él en:

https://skyone.solutions/es/legal/codigo-de-etica-y-conducta/

https://skyone.solutions/es/legal/politica-de-privacidad/

7. ¿Hay una persona DPO definida para la organización?

Sí. La información de contacto también se encuentra en nuestra página de política de privacidad en:

https://skyone.solutions/es/legal/politica-de-privacidad/

8. ¿Cuáles son las tecnologías utilizadas por Skyone?

Los entornos Skyone utilizan la última tecnología de nuestros proveedores de nube pública (Cloud Provider: AWS, Google CGP, Azure y Oracle) en Brasil y en el extranjero.

9. ¿Cuáles son las plataformas, soluciones, estándares, máquinas, conmutadores/cortafuegos que componen el entorno Skyone?

Una base importante para aquellos que consumen servicios de proveedores de nube pública es la abstracción de la capa de hardware, almacenamiento, red y virtualización.
Estos proveedores de servicios son responsables de las actualizaciones y la mitigación de riesgos.

Hardware

Aunque probablemente piense que las nubes son virtuales, requieren hardware como parte de la infraestructura, que se compone de una variedad de hardware físico que se puede ubicar en varias ubicaciones geográficas. El hardware incluye equipos de red como conmutadores, enrutadores, cortafuegos y equilibradores de carga, matrices de almacenamiento, dispositivos de copia de seguridad y servidores.
La virtualización conecta servidores entre sí, dividiendo y abstrayendo recursos para hacerlos accesibles a los usuarios.

Almacenamiento

Dentro de una sola ubicación geográfica donde se encuentra la nube, los datos se pueden almacenar en varios discos en una sola matriz de almacenamiento, lo que garantiza un alto SLA del 99,99 %. Los sistemas de administración de almacenamiento garantizan que los datos se respalden correctamente y que se indexen para su recuperación en caso de falla de alguno de los componentes de almacenamiento.

ACERCA DE LA PLATAFORMA SKYONE AUTOSKY

Red

La red está formada por recursos físicos como conmutadores, enrutadores y otros equipos. La capa de red de las nubes públicas se clasifica en VPC (Google y AWS), VNET (Azure) y VCN (Oracle).

Una configuración típica de una red en la nube se compone de varias subredes, lo que permite definir niveles de acceso, enrutamiento y asignación de direcciones IP públicas y privadas. Esta flexibilidad a nivel de red brinda la capacidad de crear múltiples capas de aislamiento entre entornos, elementos clave para mitigar los ataques de escaneo lateral.

Virtualización

La virtualización es la tecnología que separa los servicios y funciones de TI del hardware. El software llamado hipervisor se encuentra sobre el hardware físico y abstrae los recursos de la máquina, como la memoria, la potencia informática y el almacenamiento.

Una vez que estos recursos virtuales se asignan en grupos centralizados, se consideran nubes.

10. ¿Cómo podemos validar que el proveedor de la nube realmente está realizando actividades para garantizar la seguridad y la mitigación de riesgos?

a. Los proveedores de nube pública admiten estándares de cumplimiento y certificaciones como PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 y NIST 800-17 que se auditan periódicamente.

b. Además, cuentan con certificación de cumplimiento de seguridad como ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015 y CSA STAR CCM v4.

c.También cuentan con aprobación por organismos gubernamentales en varios países como Estados Unidos (FBI, NASA, CSA, entre otros) y Brasil (TSE). En cuanto a sus estándares declarados de privacidad y protección de datos, se pueden consultar en los siguientes enlaces:
https://aws.amazon.com/pt/compliance/data-privacy-faq/
https://www.oracle.com/br/cloud/cloud-infrastructure-compliance/
https://privacy.microsoft.com/pt-br/privacystatement/
https://privacy.google.com/intl/pt-BR/businesses/compliance/

ACERCA DE LA PLATAFORMA SKYONE AUTOSKY

11. ¿Qué es el modelo de responsabilidad compartida de la nube pública?

La seguridad y el cumplimiento son responsabilidades compartidas entre los proveedores de la nube pública (AWS, Google CGP, Azure y Oracle), Skyone y el cliente. Cuando el cliente transfiere sus datos y sistemas informáticos a la nube, las responsabilidades de privacidad y seguridad se comparten entre el cliente, Skyone y el proveedor de servicios en la nube. El proveedor de la nube pública es responsable de proteger la infraestructura que respalda la nube, y Skyone y los clientes son responsables de todo lo que colocan en la nube o se conectan a la nube. Por lo general, esta diferenciación de responsabilidad se conoce como seguridad en la nube vs. seguridad de la nube.

Este modelo compartido puede ayudar a reducir la carga operativa del cliente y brindar la flexibilidad y el control necesarios para implementar su infraestructura en la nube. El proveedor de la nube pública administra y controla los componentes de la infraestructura, desde la capa de virtualización hasta la implementación de los servicios relacionados y la seguridad física de las instalaciones en las que operan los servicios. Skyone y los clientes asumen la responsabilidad y la gestión del sistema operativo (incluidas las actualizaciones y los parches de seguridad), los servicios de base de datos, las aplicaciones de software asociadas con el entorno, así como el grupo de seguridad directamente vinculado a estos componentes del entorno.

ACERCA DE LA PLATAFORMA SKYONE AUTOSKY

12.¿Cómo funciona la plataforma Skyone Autosky?

Skyone Autosky es una plataforma de automatización y orquestación de recursos de múltiples nubes que facilita la migración de sistemas cliente-servidor a la nube. Además de permitir la migración de aplicaciones cliente-servidor desde todos los lenguajes de programación y diferentes bases de datos, ofrece una seguridad mucho más robusta que el hosting convencional, con copias de seguridad recurrentes realizadas de forma segura y una recuperación rápida y efectiva ante desastres.

La plataforma Skyone Autosky orquesta la creación y finalización de servidores efímeros, que son servidores creados temporalmente para atender el uso de una aplicación. Estos servidores tienen direcciones IP diferentes y de corta duración, lo que permite mitigar los ataques de fuerza bruta.with different temporary IP addresses, mitigating brute force attacks.

Si desea obtener una comprensión más profunda, puede solicitar el documento de Preguntas Frecuentes - Skyone Autosky.

13. ¿La plataforma Skyone Autosky tiene DR (recuperación ante desastres)?

La plataforma Skyone Autosky cuenta con medidas de resiliencia para garantizar su funcionamiento en caso de desastres. Al ser una aplicación nativa de la nube, se ha diseñado con tecnología de última generación que le permite ser resiliente ante situaciones adversas. En lugar de depender únicamente de planes de contingencia (DR), la resiliencia se ha convertido en un concepto sólido y confiable en el desarrollo de aplicaciones nativas de la nube. Todos los componentes de la plataforma, incluyendo la aplicación, la base de datos, los scripts, la seguridad implícita y otras funciones sistémicas, se encuentran ubicados en dos zonas de disponibilidad diferentes, lo que garantiza la resiliencia operativa.

Es importante tener en cuenta que aunque la resiliencia mejora la capacidad de recuperación, no elimina el tiempo de recuperación objetivo (RTO) ni el punto de recuperación objetivo (RPO).

Aclaración importante:

Es importante destacar que los entornos de los clientes no tienen resiliencia por defecto. Para comprender mejor las zonas de disponibilidad y su impacto en la resiliencia de la plataforma Skyone Autosky, se recomienda visitar:
https://cloud.google.com/about/locations?hl=pt-br
https://docs.aws.amazon.com/pt_br/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html
https://www.oracle.com/br/cloud/public-cloud-regions/

14. ¿Es segura la Plataforma Skyone Autosky?

La plataforma Skyone Autosky está en constante evolución (propiedad intelectual) y en los últimos 10 (diez) años ha incorporado decenas de características únicas que permiten la orquestación automática de entornos en la nube.
La orquestación automática es uno de los grandes diferenciales de la plataforma, su funcionamiento permite que cada cliente tenga su ambiente aislado (servidores de bases de datos, plantillas y sistemas de integración, entre otros) de otros clientes.

a. ¿Cuáles son los pilares estratégicos de seguridad para mitigar los riesgos?

- Realizamos escaneos de vulnerabilidades semanales;
- Pentest semestral;
- Aplicación de parches automatizados (patch packs/fix packs).

b. ¿Cómo se lleva a cabo la gestión de acceso?

La gestión de accesos en Skyone se gestiona en el área de Gobernanza de la Seguridad.

Access is granted through requests registered by the managers of permitted areas, where access blocking, privilege limitation according to function are applied, in addition to having a frequent audit routine to review these accesses.

c. ¿Qué tipos de acceso?

- Acceso de usuario a la aplicación. Este acceso seguro no requiere una VPN y se registra para todos los usuarios que se han conectado a la aplicación. Este registro se puede emitir con fines de auditoría y el acceso se puede configurar para requerir la autenticación de doble factor (MFA) o la autenticación de inicio de sesión único (SSO) mediante el protocolo SAML;
- Acceso de administrador al Panel de Administración de Skyone Autosky Este acceso, seguro y sin necesidad de VPN, es para actividades de configuración del entorno, como añadir o quitar usuarios,añadir aplicaciones y otras actividades. Se registra con fines de auditoría y tiene MFA (autenticación de doble factor);
- A Acceso para consultores, especialistas y administradores a los servidores en los que se encuentra instalada la aplicación. Este acceso es vía VPN, con credenciales de acceso emitidas a través de tickets de soporte. Las actividades realizadas directamente dentro de los servidores no se registran.

ACERCA DE LA PLATAFORMA SKYONE AUTOSKY

d. ¿Skyone garantiza el principio de mínimo privilegio, con criterios de segregación, en el que el empleado sólo tiene acceso a lo imprescindible para realizar las actividades para las que fue contratado?

Sí, tenemos como principio la adopción de privilegios mínimos en la Plataforma Skyone Autosky y en los entornos de los clientes gestionamos de forma conjunta lo que sea aplicable. Skyone utiliza una "Bóveda de Contraseñas" en todos los accesos de sus empleados a los entornos para mitigar el riesgo de fuga de credenciales de los responsables de acceder a entornos en la nube y/o clientes.
Las rutinas para cambiar contraseñas y credenciales son parte de la política de seguridad.

e.¿Hay hardening en la plataforma Skyone Autosky?

Sí, el endurecimiento es el proceso de hacer que sus sistemas, redes, software, hardware y firmware sean más resistentes a los ataques.
Eliminación continua de características o servicios innecesarios;
Actualización continua de bibliotecas y otros componentes;
Pruebas individuales y automatizadas;

f. ¿Es seguro el desarrollo?

Sí. El desarrollo de la Plataforma Skyone Autosky sigue dos conceptos: privacidad por diseño y seguridad por defecto.

Todos y cada uno de los desarrollos se realizan en entornos segregados para desarrollo, pruebas y producción.

g. ¿Cuál es la posibilidad de un ataque de denegación de servicio o un compromiso de Ransomware en la capa de virtualización?

Como explicamos en los puntos 4 y 5 anteriores, el proveedor de la nube pública mantiene, administra y mitiga la capa de virtualización.
En la nube pública, no se han registrado incidentes de violación de la capa de virtualización en los últimos años. En caso de que esta violación ocurra en un entorno de cliente, el equipo de Operaciones de Skyone recreará el entorno en una nueva zona de disponibilidad para
cumplir con el SLA contratado.

Aclaración importante:

La responsabilidad de controlar el acceso a las aplicaciones, bases de datos y otros componentes que componen el entorno recae en el cliente y/o sus proveedores y socios. Si el acceso no cumple con las recomendaciones de seguridad de Skyone, se emitirá una Notificación de Riesgo al cliente.

15. ¿Cómo proteger el entorno del cliente?

Además de las medidas de seguridad que proporciona la plataforma Skyone Autosky, sugerimos las siguientes medidas para mitigar los riesgos:

- Adoptar un software antimalware avanzado con funciones de monitoreo y alertas de eventos de seguridad utilizando la tecnología XDR (Detección y respuesta extendida);
- Contratar el servicio de Protección de Superficies (Plataforma Seguridad Cibernética), que escanea en busca de vulnerabilidades en las superficies internas y externas;
- Mantener actualizados todos los paquetes de corrección indicados por Vulnerabilidades y Exposiciones Comunes (CVE) de Mitre para identificar, definir y catalogar las vulnerabilidades de seguridad cibernética divulgadas públicamente.

16. ¿Cómo mitigar los riesgos cuando los empleados y consultores tienen acceso para implementar, administrar y/o mantener elentorno del cliente?

Las siguientes medidas de seguridad se enumeran como mejores prácticas:

- AAdoptar EDR (Endpoint Detection and Response) para todos los portátiles (puntos finales) de empleados y consultores;
- Gestionar centralmente el acceso y cambiar constantemente las contraseñas para estos empleados;
- Adoptar VPN como estándar para el acceso remoto al entorno al implementar, administrar y/o mantener el entorno.

17. ¿Cómo está preparada la Plataforma Skyone Autosky para mitigar los riesgos en el entorno del cliente?

La evolución de la Plataforma Skyone Autosky incorporó varias funciones de seguridad y procesos de gestión destinados a mitigar los riesgos, entre ellos:

a. Reglas del cortafuegos

Se controlan a través de NSG (Network Security Group) exclusivo para cada entorno de cliente;

b. Puertos de comunicación

La liberación de puertos de comunicación con redes externas se realiza a través de análisis y cuando existen riesgos se genera una Notificación de Riesgos para dar visibilidad y concientización;

c. Operating Systems (OS) and software

By default we provide the latest versions.

d. Capa de autenticación

- SAcceso seguro a través de una URL con autenticación con ReCaptcha, MFA y Single Sign-On usando SAML.
- Todos los accesos son registrados y auditables.
- Restricciones de acceso en base a horarios e IPs.
- Configuración para definir patrones de contraseñas (caracteres y longitudes)

ACERCA DE LA PLATAFORMA SKYONE AUTOSKY

e. Escalado de aplicaciones

La Plataforma gestiona diariamente los servidores del entorno de forma dinámica, asegurando IP's dinámicas, mitigando los ataques de fuerza bruta. Este mismo mecanismo se utiliza en el servidor de plantillas (que es la matriz de referencia para la creación de entornos de usuario).

f. Supervisión

Monitoreo 24×7, con visualización de cuadros de mando a disposición de los clientes.

g. Contra software malicioso (Anti Malware)

Versión básica instalada en todos los entornos (versión avanzada disponible como opción).

h. Prevention of brute force attacks

Para mitigar los ataques de fuerza bruta, creamos Skyone Autosky Defender, que monitorea y mitiga los ataques en tiempo real, bloqueando las IP infractoras, centralizando el análisis de las IP y permitiendo el bloqueo de bloques completos.

i. Auditoría

La Plataforma registra todas las acciones del usuario realizadas en el portal del usuario, tales como:

- Intentos de acceso;
- Autenticación fallida;
- Intentos de inicio de sesión fallidos excesivos limitan con el bloqueo del usuario;
- Recuperación de contraseña y
- Cambio de contraseña

18. ¿Sobre el proceso de respaldo para clientes en la Plataforma Skyone Autosky?

El backup es el proceso de realizar copias de seguridad de un entorno, aplicación o datos de un cliente en un momento determinado. Consiste en hacer copias en diferentes dispositivos de almacenamiento para recuperar el sistema en caso de fallas.

¿Cuál es la política de copia de seguridad predeterminada de Skyone Autosky?

a. La política de backup por defecto para cualquier entorno de cliente es una instantánea de la instancia y el servidor con base de datos, con una retención de 7 (siete) días..

b. Hay otras opciones de granularidad, retención y destino de respaldo que pueden ser configuradas.

¿Cómo se evidencia la realización de respaldos?

Todos los clientes de Skyone tienen acceso al Portal del Cliente, donde encontrarán una lista de las copias de seguridad realizadas por entorno/servidor.

¿Cómo solicito la recuperación de una copia de seguridad?

La recuperación de copias de seguridad se realiza a través del Panel de Clientes, en la lista de copias de seguridad. Existe una opción para solicitar la recuperación que abre automáticamente un ticket.

¿Cuál es el procedimiento de prueba de recuperación de copia de seguridad de Skone?

El cliente puede solicitar, a través de un ticket abierto en nuestro Portal de Clientes, la creación de un entorno recuperado para llevar a cabo las pruebas necesarias.

¿Cómo se almacenan las copias de seguridad?

a. De forma predeterminada, las instantáneas se almacenan en el área de almacenamiento de objetos de las cuentas activas de los clientes, que tienen una gran capacidad de recuperación, en el servidor de la nube pública. Todas las copias de seguridad se almacenan en AWS Simple Storage Service (S3), OCI Object Storage, Azure Object Storage o Google Cloud Storage. Las copias de seguridad se replican automáticamente entre varias zonas, lo que garantiza una durabilidad del 99,999999999%.

b. Las áreas de almacenamiento de objetos están aisladas de los servidores, sin conexión directa entre ellos. En caso de compromiso del servidor, no hay acceso a las instantáneas almacenadas.

c. Además, las copias de seguridad en OCI se cifran automáticamente antes del almacenamiento en Object Storage. Storage.

Para obtener más detalles, puede solicitar el documento: Skyone Backup Policy Version: 4.0 - Enero 2022

ACLARACIÓN DE LAS PRÁCTICAS DE PRIVACIDAD, PROTECCIÓN DE DATOS Y CIBERSEGURIDAD DE SKYONE

Lauro de Lauro
COO

Cristiane Santos
Gerente de Gobernanza
DPO

Control de versiones y cambios

Versión	Emisíon		Description	Revisión / Liberar	
	Fecha	Responsable		Fecha	Responsable
1.0.0	05.04.2023	Cristiane Santos	Elaboración del documento inicial	13.04.2023	Caetano Notari
1.1.0	17.04.2023	Angelo Ferreira Anunziato	Revisión de maquetación y textos	17.04.2023	Lauro de Lauro
1.2.0	17.04.2023	Angelo Ferreira Anunziato	Revisión de maquetación y textos	17.04.2023	Caetano Notari

Traducido por ChatGPT

skyone

Una plataforma. Infinitas posibilidades.

Av. Nações Unidas 12399 - São Paulo, SP
+55(11) 2193-1961
www.skyone.solutions