

HELISA Software para el trabajo	PROASISTEMAS S.A.	Código: TI-PT-001
	Política de Seguridad de las Operaciones: Copias de Respaldo	Versión: 01 Fecha: 24/08/2018 Página 1 de 5

Política de Seguridad de las Operaciones: Copias de Respaldo

1. Objetivo

Establecer los lineamientos para asegurar que toda la información almacenada en nuestros servidores de clientes Helisa Cloud y Hosting se pueda respaldar, almacenar y recuperar, garantizando que la información esté disponible y pueda ser restaurada en caso de una falla o solicitud por parte de los clientes.

2. Alcance

Las políticas descritas en este documento aplican para todos los clientes de Helisa Cloud y Hosting, que tengan un servicio o contrato vigente con Proasistemas S.A.

En concordancia con lo anterior se contemplan los siguientes lineamientos:

3. Centro de Datos

Los servicios de acceso y almacenamiento son brindados por nuestro proveedor de servicios de Datacenter HostDime cuyo centro de datos DC2 se encuentra ubicado en Orlando Florida (USA) el cual cuenta con instalaciones totalmente restringidas, contando con controles de acceso con tecnología de punta:

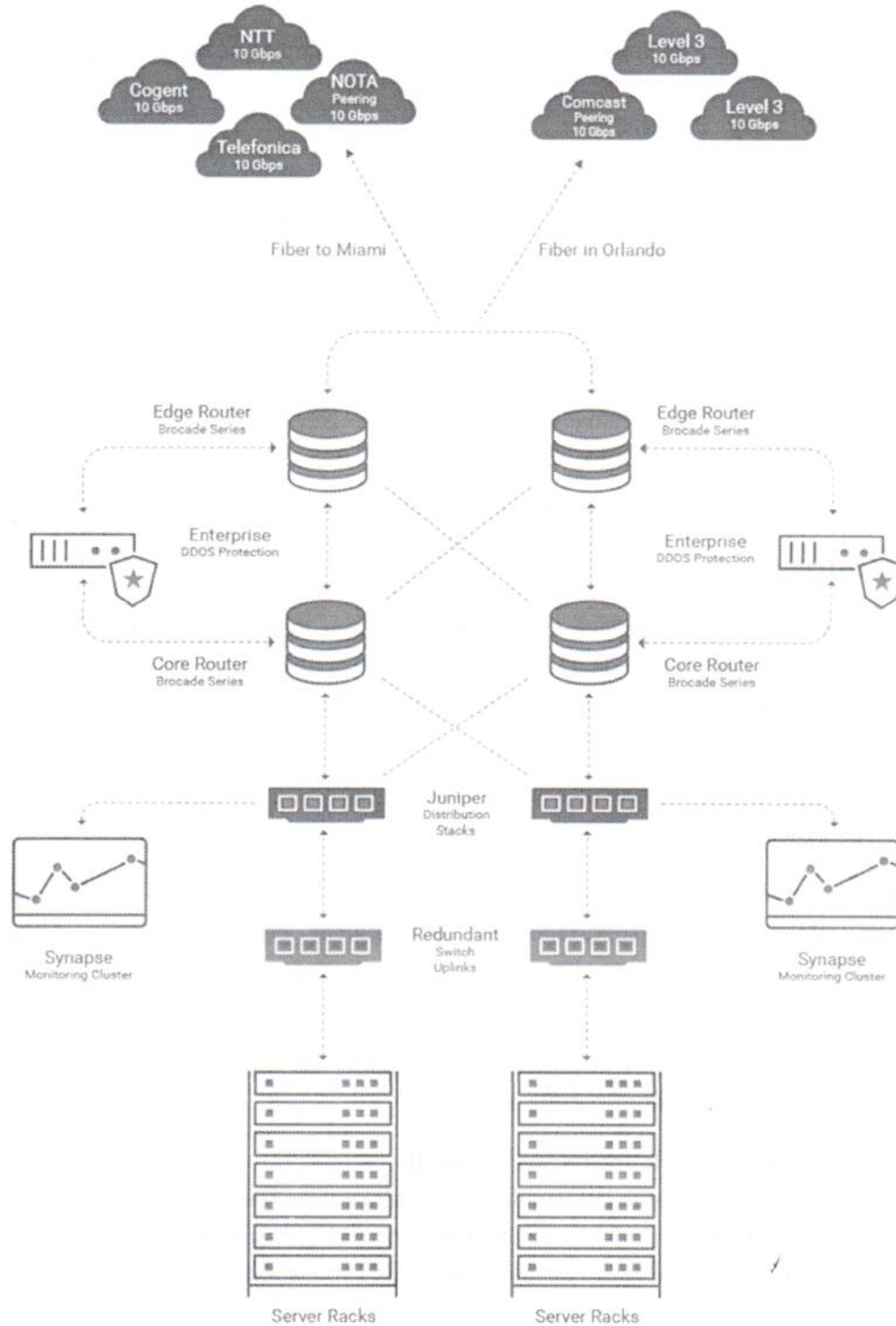
- Tarjetas magnéticas
- Sensores biométricos

Además de un sistema de CCTV que nos permite garantizar altos niveles de seguridad para los equipos de información. Es soportado por los sistemas de energéticos y ambientales completamente redundantes.

Al ser un proveedor líder de centros de datos globales, mantiene la privacidad y seguridad del cliente por encima de todo. En consecuencia, demuestra las mejores prácticas al lograr las siguientes certificaciones de cumplimiento:

- SOC 2 tipo 2 (anteriormente SAS 70 tipo II).
- Las instalaciones están construidas con características Tier III.
- Protección DDOS, mediante el cual todos los clientes están en red segura, por lo que sus sitios están protegidos de los ataques DDoS con la red más.

3.1. Topología de Red Centro de Datos Orlando Florida (USA)



Este documento es propiedad intelectual de Proasistemas S.A., y queda prohibida su reproducción total o parcial en cualquier medio. El otorgamiento de una copia a terceros, deberá ser con autorización escrita de la gerencia o en su defecto el responsable de Proasistemas S.A.

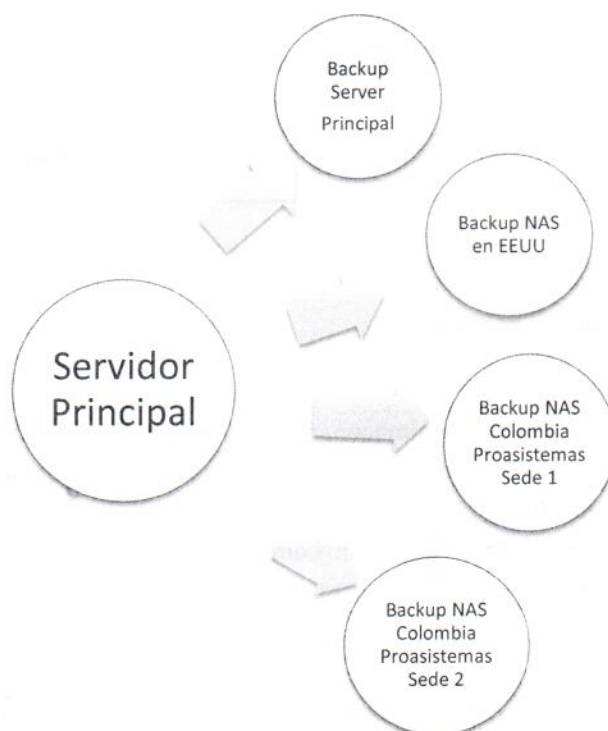
4. Copias de Respaldo (Proasistemas)

La seguridad de la información es una de las más altas prioridades en Proasistemas ya que conocemos los riesgos a los que está sometida su información los cuales minimizamos y controlamos mediante un sistema de gestión de copias de seguridad el cual permite poder brindar a nuestros clientes tranquilidad en el almacenamiento de la información y con ello lograr prevenir inconvenientes futuros.

Las copias de seguridad se han convertido en la herramienta más importante para sobrellevar algún tipo de ataque o catástrofe que cause pérdida de información en las compañías, es por ello por lo que para nuestros clientes de Helisa Cloud y Hosting manejamos un protocolo específico para los respaldos de información.

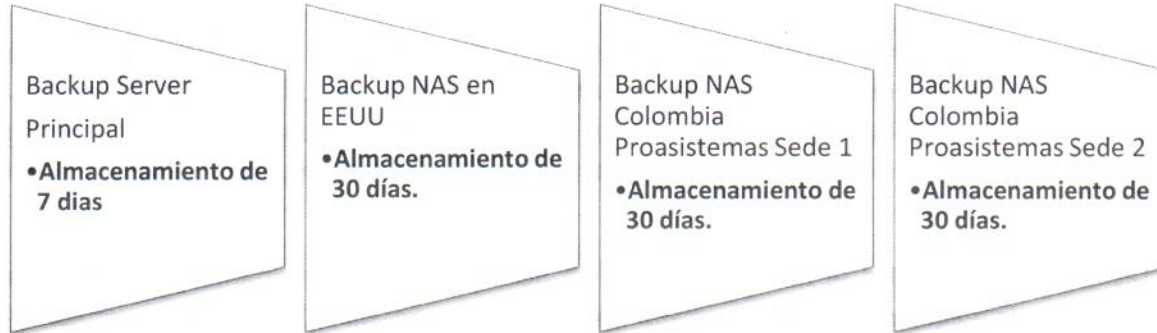
Nuestras copias de seguridad son realizadas sobre la carpeta donde se encuentran almacenadas las bases de datos que se trabajan en la licencia que maneja su compañía, cabe aclarar que a la carpeta de acceso FTP asignada no se le genera ningún tipo de respaldo de información por ser de paso transitorio.

Como se muestra a continuación nuestra estructura de copias de seguridad genera redundancia en 4 puntos diferentes a nivel mundial lo que permite contar con excelente respaldo de la información.



4.1. Tiempo de almacenamiento

El almacenamiento de las copias de seguridad está limitada a tiempos específicos los cuales se relacionan en la siguiente imagen.



4.2. Horarios de Generación de Copias de Respaldo

Con el fin de garantizar un respaldo de la información efectivo se han determinado horarios específicos para realizar su respectiva generación:

CLIENTES TERMINALES CON NUMERACIÓN PAR	CLIENTES TERMINALES CON NUMERACIÓN IMPAR	CLIENTES CLINICAS
Reinicio de servidor 12 de la noche	Reinicio de servidor 1 am	Reinicio de servidor 1 am
Generación Copias 2 am	Generación de Copias 3am	Generación de Copias 3am
Diariamente	Diariamente	Diariamente

4.3. Solicitud de una copia de respaldo

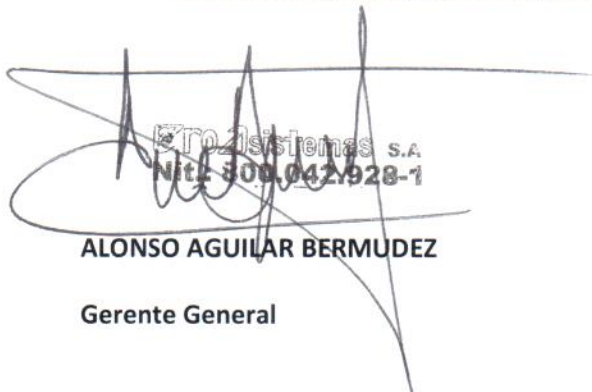
En caso de requerir copias de seguridad almacenadas en los centros de datos establecidos por Proasistemas, se debe enviar un correo electrónico firmado por el representante legal de la empresa al correo electrónico helisacloud@helisa.com, indicando la fecha (día) de la cual se requiere generar la copia de respaldo, el tiempo máximo de respuesta por parte de Proasistemas es de 24 horas hábiles después de recibir la solicitud.

4.4. Copias de Respaldo (Clientes)

Como se especifica en este documento Proasistemas brinda a los clientes la seguridad en el almacenamiento de copias de respaldo de la información, sin embargo ofrece la posibilidad directamente en la herramienta Helisa de generar copias de seguridad de forma manual y con ello brindar a nuestros clientes la posibilidad de almacenar sus propias copias de seguridad en sus centros de datos o dispositivos de almacenamiento. En caso de requerir información adicional para realizar este proceso comuníquese con nuestro equipo de soporte para solicitar una instrucción al respecto.

5. Glosario:

- **Backup:** Copia de seguridad de los archivos almacenados en una computadora.
- **Copia de Respaldo:** Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **DC2:** Centro de Datos Secundario de respaldo del proveedor del Data Center.
- **NAS:** Nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red.
- **Protección DDOS:** Protección contra ataques a un servidor u ordenador desde muchos equipos a la vez.
- **SOC 2 tipo 2:** Es la certificación otorgada a organizaciones de servicios, particularmente en las áreas de Tecnología y Cloud Computing, demuestran tener implementados los más rigurosos controles de seguridad y seguimiento las mejores prácticas, diseñados para proteger efectivamente los sistemas de información contra el uso inapropiado y el acceso o modificación, sin la debida autorización.
- **Tier III:** Corresponden a las garantías que ofrecen en cuanto al tipo de hardware que utiliza el Datacenter para garantizar su redundancia. Un Datacenter Tier III ofrece una disponibilidad del 99,98%. Con esta configuración, existe la posibilidad de programar periodos de mantenimiento sin que afecten a la continuidad del servicio en los servidores



Proasistemas S.A.
Nit: 800.042.928-1

ALONSO AGUILAR BERMUDEZ

Gerente General