# IMPLEMENTACIÓN DE SEGURIDAD EN LOS EQUIPOS DE RED

Para garantizar la seguridad de los equipos de red, se han implementado las siguientes medidas:

* Sesiones SSH: Todos los equipos de red (switches y routers) han sido configurados para permitir únicamente conexiones seguras a través del protocolo SSH.

Se han establecido requisitos de complejidad para las contraseñas de acceso SSH, incluyendo una longitud mínima de 8 caracteres y la combinación de letras mayúsculas, minúsculas, números y caracteres especiales.

Las sesiones SSH cuentan con un tiempo de espera de inactividad de 5 minutos, lo que obliga a los usuarios a volver a autenticarse después de un período de inactividad.

* Contraseñas de Consola: Todas las contraseñas de consola han sido modificadas de los valores predeterminados y cumplen con los requisitos de complejidad mencionados anteriormente.

El acceso a la consola local de los equipos de red se restringe únicamente a personal autorizado.

* Encriptación de Contraseñas: Todas las contraseñas almacenadas en los equipos de red están encriptadas utilizando algoritmos seguros, como SHA-256.

No se permiten contraseñas en texto plano en ninguno de los dispositivos.

Banners de Advertencia: Se han configurado banners de advertencia en los equipos de red, informando a los usuarios sobre las políticas de uso y seguridad de la red.

Estos banners se muestran al iniciar sesión a través de SSH o la consola local.

* Monitoreo y Registro: Se ha habilitado el registro de eventos (logging) en todos los equipos de red, lo que permite la auditoría y el análisis de actividades sospechosas.

Los registros se envían a un servidor central de gestión de registros (syslog) para su almacenamiento y monitoreo.

Estas medidas de seguridad implementadas en los equipos de red tienen como objetivo proteger la infraestructura de red contra accesos no autorizados, garantizar la integridad de la información y facilitar la detección y respuesta ante posibles incidentes de seguridad.