PROGRAMA MODULAR EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

PRÁCTICO

Proyecto

Diseño e Implementación de Infraestructura de Seguridad para Consultoría legal con Enfoque en Ciberseguridad y Trabajo Remoto

Alumna: **Mercedes Cea Rodríguez**

Tutora: **Elena Ruiz Larrocha**

AGRADECIMIENTOS

Quisiera expresar mi profundo agradecimiento a aquellos que desempeñaron un papel fundamental en la realización y conclusión exitosa de mi proyecto académico titulado "Diseño e Implementación de Infraestructura de Seguridad para Consultoría Legal con Enfoque en Ciberseguridad y Trabajo Remoto". Este proyecto representó no solo un desafío técnico significativo, sino también un viaje personal de crecimiento y aprendizaje.

En primer lugar, extiendo mi gratitud a mi familia, cuyo apoyo incondicional y aliento constante fueron el cimiento sobre el cual construí este logro. Su comprensión durante las extensas horas dedicadas al estudio y al desarrollo del proyecto ha sido un faro que iluminó mi camino.

Mi reconocimiento especial se dirige al profesor de ciclo, Manuel Melero, cuya dedicación trasciende los confines de lo académico. Su disposición para conectar más allá de las horas lectivas, incluso en fines de semana, marcó la diferencia al brindar orientación experta y apoyo crucial en los aspectos más desafiantes de la ciberseguridad y el diseño de infraestructuras.

A la tutora del proyecto, Elena Ruiz Larrocha, le debo una deuda de gratitud por sus consejos perspicaces, su paciencia infinita y su orientación especializada. Su influencia fue crucial en la configuración de la dirección y el alcance del proyecto, así como en mi propio desarrollo académico y profesional.

Al director del ciclo, Agustín Carlos Caminero Herráez, agradezco su pronta respuesta y compromiso constante con el éxito de los estudiantes. Su liderazgo ha proporcionado un entorno propicio para el aprendizaje y la consecución de metas académicas.

La complejidad de este ciclo formativo se vio agravada por una carga laboral exigente, responsabilidades familiares y la asimilación de conceptos avanzados. Sin embargo, el desafío se convirtió en una oportunidad gracias al apoyo integral del profesorado y de todos aquellos que contribuyeron a mi formación.

Este proyecto no solo representa la culminación de una tarea académica, sino también la apertura de nuevos horizontes tanto en términos técnicos como humanos. La oportunidad de diseñar e implementar una infraestructura de seguridad en el contexto de la consultoría legal, con especial énfasis en la ciberseguridad y el trabajo remoto, ha ampliado mi perspectiva de manera significativa.

En conclusión, a cada persona que ha formado parte de este viaje académico, les agradezco sinceramente por creer en mí y por contribuir de manera esencial a este logro. Este proyecto no solo representa un hito en mi formación, sino también un testimonio de la colaboración y el esfuerzo conjunto que caracterizan a una educación de calidad por parte de la UNED[1]. Gracias por hacer posible este capítulo significativo en mi desarrollo académico y profesional.

[1] UNED, siglas de la Universidad Nacional de Educación a Distancia

Índice de contenido

Índice de figuras

1. Resumen/Abstract

Este proyecto propone una infraestructura de red robusta y segura con un enfoque integral en varios aspectos clave. La topología de la red incluirá un direccionamiento fijo privado, un firewall, switches, routers, servidores de dominio y archivos, así como un SIEM (*Security Information and Event Management*) para la gestión de eventos de seguridad. Además, se implementará un NAS para un almacenamiento centralizado y una consola para facilitar la administración y supervisión.

En términos de conectividad, se emplea cableado UTP (*Unshielded Twisted Pair*) para asegurar una conexión confiable. Se destacan las VPNs (*Virtual Private Network*) como una medida esencial para prevenir ataques de ransomware y garantizar la seguridad de la información, mientras que la virtualización se utilizará para optimizar recursos y mejorar la flexibilidad operativa.

La sala de reuniones estará tecnológicamente equipada, con características como tecnología VoIP (*Voice over Internet Protocol)* una pantalla conectada a un interruptor versátil y la capacidad para realizar reuniones virtuales. Este enfoque mejora la colaboración tanto interna como remota.

La adopción de políticas pro-BYOD (*Bring Your Own Device*) para empleados, clientes y accionistas promoverá la flexibilidad y modernidad en el entorno laboral. Además, se implementarán medidas de seguridad avanzadas, como protección contra DDoS (*Distributed Denial of Service)* para garantizar la disponibilidad de los servicios y acceso biométrico en la entrada de la empresa para fortalecer la seguridad.

El compromiso con la norma ISO 27001 (*International Stardard Organization*) destaca el enfoque proactivo hacia la seguridad de los datos. La implementación de medidas específicas garantizará la alineación con esta norma reconocida, asegurando así la integridad y confidencialidad de la información.

En resumen, este proyecto busca establecer una infraestructura de red segura y moderna que abarque desde la topología de red hasta medidas específicas de seguridad, promoviendo la flexibilidad y la colaboración en el entorno empresarial, y cumpliendo con estándares internacionales de seguridad de datos.

This project proposes a robust and secure network infrastructure with a comprehensive focus en key aspects. The network topology will include a private fixed addressing, a firewall, switches, routers, domain servers, and file servers, along with a Security Information and Event Management (SIEM) system for security event management. Additionally, a Network Attached Storage (NAS) will be implemented for centralized storage, and a console will facilitate administration and monitoring.

In terms of connectivity, an Unshielded Twisted Pair (UTP) cabling will be employed to ensure a reliable connection. Virtual Private Networks (VPNs) are highlighted as an essential measure to prevent ransomware attacks and ensure information security, while virtualization will be used to optimize resources and enhance operational flexibility.

The technologically equipped meeting room features Voice over Internet Protocol (VoIP) technology, a screen connected to a versatile switch, and the capability for virtual meetings. This approach improves collaboration both internally and remotely.

The adoption of pro-BYOD (Bring Your Own Device) policies for employees, clients, and shareholders will promote flexibility and modernity in the workplace. Additionally, advanced security measures, such as DDoS protection to ensure service availability and biometric access at the company entrance, will be implemented.

Commitment to the ISO 27001 standard underscores the proactive approach to data security. The implementation of specific measures will ensure alignment with this recognized standard, thus guaranteeing the integrity and confidentiality of information.

In summary, this project aims to establish a secure and modern network infrastructure, covering everything from network topology to specific security measures, promoting flexibility and collaboration in the business environment, and complying with international data security standards.

2. Antecedentes/Introducción

En la era digital, donde la gestión segura de datos sensibles se ha convertido en imperativo, la necesidad de robustecer la infraestructura de red se vuelve esencial para cualquier organización. En particular, las consultorías legales, guardianas de información confidencial de clientes, se enfrentan a desafíos significativos en la era del trabajo remoto.

Este proyecto surge como respuesta a la creciente brecha de seguridad en la mayoría de las empresas, muchas de las cuales subestiman la importancia de invertir en la protección de la información. En un mundo donde las cibercrisis son una realidad, nuestro enfoque es proactivo. Mostraremos cómo transformar e impulsar la seguridad de la información, destacando herramientas y métodos para mitigar y prevenir ataques, como los que han afectado a empresas notables, incluyendo el incidente de Ransomware en Garmin.

Nos adentraremos en la creación de una infraestructura de red segura y resiliente, con un enfoque práctico y aplicable a diversos sectores empresariales. Este proyecto, inicialmente basado en un escenario de consultoría legal, es extrapolable a instituciones financieras, empresas industriales y más. La diferencia radica en la rigurosidad de las auditorías de seguridad necesarias para demostrar la confiabilidad de la infraestructura ante clientes, empleados y accionistas.

Investigaremos cómo implementar, no solo una red segura, sino una cultura de seguridad arraigada en la prevención y mitigación de amenazas cibernéticas. Este enfoque no solo protege los activos de la empresa, sino que también refuerza la confianza de todas las partes interesadas. Conozcamos juntos el camino hacia una infraestructura de seguridad que no solo cumple con estándares, sino que establece nuevos estándares de confianza y resiliencia.

Se espera que este proyecto contribuya a mantener el crecimiento y la seguridad de una empresa con un ROE[2] del 20% y un beneficio anual de 3 millones de euros.

Se proporcionarán planos detallados de la empresa para visualizar la implementación propuesta. Este elemento será fundamental para guiar la ejecución del proyecto y facilitar la comprensión de la nueva infraestructura.

En el contexto actual de rápida evolución tecnológica y creciente sofisticación de las amenazas cibernéticas, es imperativo para la empresa que nos encomienda el proyecto, una evaluación integral de su postura actual.

La empresa que tiene una superficie de 300m2 y que cuenta con un equipo de 21 empleados en sus instalaciones, más 38 que lo hacen de forma remota, se enfrentarán a desafíos particulares en la protección de activos digitales y la garantía de la continuidad operativa.

[2] ROE, siglas del inglés "*Return on Equity*", que se utiliza como medida financiera para evaluar la rentabilidad de una empresa en relación con el patrimonio neto de los accionistas.

Hasta la fecha, han implementado ciertas medidas de seguridad como firewalls, antivirus. Sin embargo, la rápida expansión del trabajo remoto y la evolución constante de las amenazas cibernéticas requieren una revisión más profunda de nuestra estrategia de seguridad.

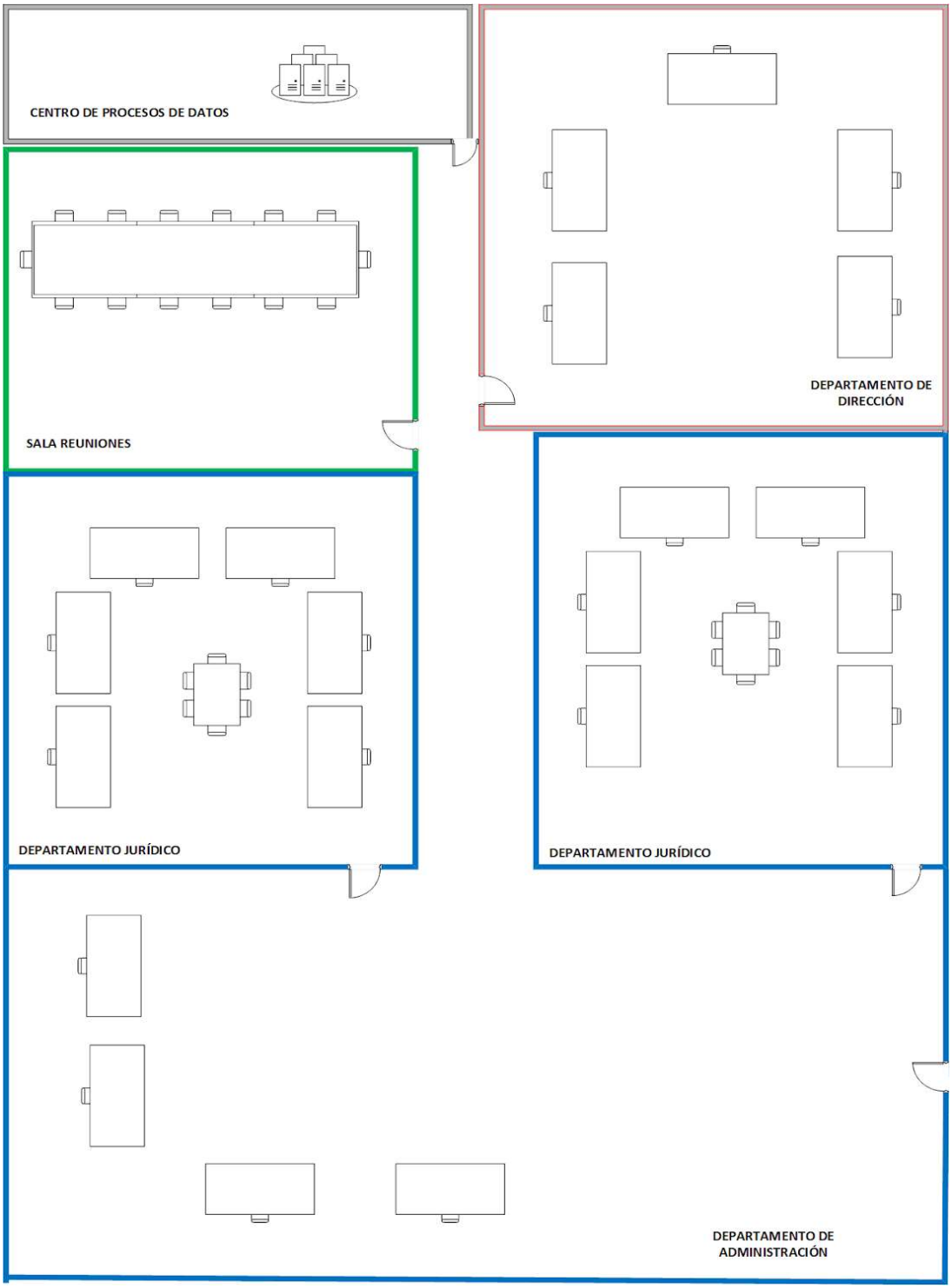

Ilustración 1. Plano de la empresa. Fuente: Propia

3. Objetivos generales y específicos y alcance del proyecto

Objetivos generales

Este proyecto busca no solo fortalecer la infraestructura tecnológica, sino también posicionar a la empresa como un referente en adaptabilidad, seguridad y eficiencia. A través de estos objetivos, aspiramos a construir un futuro empresarial sólido y preparado para los desafíos venideros. Por este motivo, la implementación de una infraestructura de red y seguridad sólida es esencial para garantizar la eficiencia operativa, la seguridad de la información y la adaptabilidad a los desafíos futuros. Este proyecto tiene como objetivo principal diseñar y poner en marcha una infraestructura tecnológica que no solo cumpla con los estándares de seguridad más rigurosos, sino que también promueva la flexibilidad, la colaboración y la eficiencia en todos los aspectos de nuestras operaciones.

Objetivos específicos

En el marco de nuestra iniciativa para fortalecer la infraestructura tecnológica y la seguridad de la información, se han definido objetivos específicos que abordan aspectos cruciales para alcanzar nuestras metas generales. Estos objetivos detallados se centran en áreas específicas que contribuirán directamente al éxito de nuestro proyecto, asegurando una implementación robusta y eficiente.

Seguridad Integral:

- Implementar un sistema de prevención de intrusiones (IPS) para detectar y bloquear amenazas cibernéticas.
- Establecer políticas de seguridad de contraseñas y autenticación de dos factores para acceder a sistemas críticos.

Alta Disponibilidad:

- Configurar un sistema de clustering para los servidores críticos, permitiendo la conmutación por error sin pérdida de datos.
- Realizar simulacros regulares de recuperación de desastres para evaluar la efectividad de los procedimientos.

Virtualización Eficiente:

- Utilizar herramientas de gestión de virtualización para optimizar la asignación de recursos y monitorizar el rendimiento de las máquinas virtuales.
- Implementar una política de aprovisionamiento dinámico para ajustar automáticamente los recursos según la demanda.

Redes Seguras y Eficientes:

- Configurar reglas de firewall específicas para cada VLAN, controlando el tráfico de red según las políticas establecidas.
- Realizar auditorías periódicas de seguridad de red para identificar posibles vulnerabilidades y aplicar correcciones.

Acceso Remoto Seguro:

- Implementar autenticación multifactor (MFA) para el acceso remoto, mejorando la seguridad de las conexiones.
- Configurar políticas de acceso remoto basadas en roles para garantizar permisos adecuados.

Tecnología en Sala de Reuniones:

- Instalar sistemas de videoconferencia de alta calidad para facilitar reuniones virtuales efectivas.
- Integrar soluciones de gestión de presentaciones para mejorar la eficiencia durante las sesiones.

Cumplimiento Normativo:

- Realizar auditorías internas y externas periódicas para verificar el cumplimiento con estándares y regulaciones.
- Documentar y mantener actualizadas las políticas y procedimientos de seguridad de acuerdo con los requisitos normativos.

Monitoreo Continuo:

- Implementar herramientas de monitoreo de seguridad en tiempo real para detectar y responder a eventos anómalos.
- Establecer alertas y notificaciones automáticas para abordar problemas críticos de manera proactiva.

Escalabilidad y Planificación a Futuro:

- Diseñar la arquitectura de red para admitir fácilmente la incorporación de nuevos empleados y dispositivos.
- Evaluar y actualizar periódicamente la capacidad de almacenamiento y procesamiento para anticipar el crecimiento.

Políticas de BYOD:

- Desarrollar directrices claras sobre los dispositivos permitidos y las medidas de seguridad necesarias para los dispositivos personales.
- Implementar soluciones de gestión de dispositivos móviles (MDM) para garantizar el cumplimiento de las políticas BYOD.

4. Definiciones

Clúster se refiere a un grupo de ordenadores o nodos interconectados que trabajan juntos como si fuesen una única unidad. Estos nodos están diseñados para colaborar en la ejecución de tareas y compartir la carga de trabajo. Se utilizan para mejorar el rendimiento, la disponibilidad y la escalabilidad en diversas aplicaciones y entornos. (ela)

Firewall, en español "cortafuegos", es una barrera de seguridad que ese utiliza para proteger los ordenadores o un sistema informativo contra accesos no autorizados, ataques cibernéticos y otros riesgos de seguridad. Su principal función es regular y controlar el tráfico de datos entre una red interna privad ay redes externas, como internet. (Fernández, 2019)

Hyper-V es una plataforma de virtualización desarrollada por Microsoft que se utiliza para crear y gestionar maquina virtuales (VM) en entornos de sistemas operativos Windows. Permite que múltiples sistemas operativos se ejecuten en un solo servidor físico, compartiendo eficientemente los recursos de hardware. (colaboradores, 2023)

Palo Alto es una empresa especializada en soluciones de seguridad cibernética. (pal)

Ransomware es un tipo de software malicioso (malware) para cifrar los archivos en un equipo o sistema y luego exigir un rescate (un pago) al propietario del sistema para restaurar el acceso a los archivos. Este tipo de extorsión no asegura su restauración. (ibm)

Router es un dispositivo de red que se utiliza para conectar y dirigir el tráfico de datos entre diferentes redes. Su función principal es determinar cuál es la mejor ruta para enviar paquetes de datos desde la red de origen hasta su destino a través de la red. (Burdova, 2022)

Servidor de archivos es un servidor que proporciona acceso centralizado a archivos y recursos compartidos en una red, como impresoras. (Marujita, 2023)

Servidor de dominio es un servidor que gestiona y controla el acceso a los recursos en un domino de red. Se utiliza en redes que opera n con el protocolo de Directorio Activo de Microsoft (*Active Directory*). (wik)

Switch, en español es un conmutador de red que opera en la capa 2 de enlace de datos del modelo OSI y se utiliza para conectar dispositivos dentro de una red local (LAN). (Herrera, 2022)

5. Notaciones y símbolos

AWS *(Amazon Web Services)* es una plataforma de servicios en la nube proporcionada por Amazon. Se lanzó en 2006 y ha crecido para convertirse en uno de los proveedores líderes de servicios en la nube a nivel mundial. (aws.amazon)

ACL significa "*Access Control List*" en inglés, se traduce como lista de control de acceso. Es una lista que especifica los permisos de acceso a recursos, archivos o servicios para usuarios o sistemas. Se utiliza para gestionar quién tiene acceso y qué tipo de acceso tiene. (vasexperts)

BYOD, que significa **"***Bring Your Own Device*" en inglés, se traduce como "Trae Tu Propio Dispositivo". Este término se refiere a una política o practica en la que los empleados utilizan sus propios dispositivos personales, como teléfonos inteligentes, tabletas, ordenadores portátiles y otros dispositivos, para realizar tareas laborales y acceder a los recursos de la empresa. (ionos)

CPD son las siglas que corresponden a "Centro de Proceso de Datos", que es una instalación o lugar físico diseñado para albergar y gestionar sistemas informativos, servidores, equipos de almacenamiento, redes y otros componente relacionados con el procesamiento y gestión de datos. (34, Grupo Atico)

DDoS significa "*Distributed Denial of Service*" en inglés, y en español se traduce como "Ataque de Denegación de Servicio Distribuido". Es un tipo de ciberataque en el que múltiples sistemas informáticos son utilizaos para inundar, abrumar o saturar los recursos de un sistema objetivo, con un servidor o una red, con el objetivo de dejarlo fuera de servicio, provocando una denegación de servicio para los usuarios legítimos. (akami)

DHCP son las siglas de "Dynamic Host Configuration Protocol" en inglés, y en español se traduce como "Protocolo de Configuración Dinámica de Host". Es un protocolo de red que se utiliza para asignar de manera dinámica direcciones IP y otros parámetros de configuración de red a dispositivos en una red, como ordenadores, impresoras y otros dispositivos conectados. (wikipedia)

IP (Internet Protocol) es un número único asignado a cada dispositivo conectado a una red que utiliza el protocolo de internet para las comunicaciones. Las direcciones IP son esenciales para que los dispositivos puedan identificarse y comunicarse entre sí en una red. (ionos)

ISO 27001, son las siglas en ingles de "*International Standard Organization*"**.** Es una norma internacional que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) dentro del contexto de los riesgos generales del negocio. La norma está diseñada para ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que poseen. (Editorial, 2023)

NAS, por sus siglas en inglés, se refiere a "*Network Attached Storage*" en español, "Almacenamiento Conectado a la Red". Es un tipo de dispositivo de almacenamiento dedicado

a proporcionar servicios de almacenamiento de datos a través de una red, permitiendo que múltiples usuario y sistemas accedan y compartan archivos de manera centralizada. (ibm)

SIEM son las siglas del inglés “Security Information and Event Management”, que se traduce a español como “Gestión de Información y Eventos de Seguridad”. Proporciona una visión unificada de la seguridad del entorno informático. (ibm)

UTP son las siglas del inglés "Unshielded Twisted Pair", que en español se traduce como "Par Trenzado No Apantallado". Es un tipo de cable utilizado comúnmente en redes de telecomunicaciones y de equipos informáticos. (wikipedia, 2023)

VoIP son las siglas de “*Voice over Internet Protocol”* en inglés, que se traduce como “Voz sobre Protocolo de Internet” en español. Esta tecnología permite realizar llamadas de voz, y en algunos casos, transmitir otros tipos de medios a través de redes de internet en lugar de las redes telefónicas tradicionales. (gesditel)

VLAN, siglas en inglés “*Virtual Local Area Network*”, que se traduce en español como “Red Virtual de Área Local”, es un sistema que permite creación de redes lógicas independientes dentro de una misma red física. (guiaspracticas)

VPN son las siglas del inglés “*Virtual Private Network”,* que se traduce en español como “Red Privada Virtual”. Es una tecnología que crea una conexión segura y encriptada entre redes a través de internet. (Empey & Latto, 2023)

WAN son las siglas "*Wide Area Network*" en inglés, que se traduce al español como "Red de Área Amplia". Una WAN es una red de equipos que abarca un área geográfica extensa, como una ciudad, un país o incluso a nivel mundial. (capterra)

6. Desarrollo del trabajo final

6.1. ISO 27001 y Seguridad de Datos

Se aplicará la norma ISO 27001 que establece un marco para la implementación del nuestro sistema de gestión de la seguridad de la información que se basará en el riesgo para proteger la información.

Se identificarán y evaluarán los riesgos de seguridad de la información. Para ello, se documentarán las posibles amenazas ya sean internas, externas, vulnerabilidades del sistema, cambios en el entorno operativo, entre otros.

Una vez identificados los riesgos, realizaremos una evaluación para determinar la probabilidad de que ocurran y el impacto que tendrían en la seguridad de la información y más concretamente en la seguridad de nuestros datos. Con esta acción, habiendo evaluado riesgos los trataremos para ver qué solución factible dar, ya sea aceptar el riesgo, mitigarlo, transferirlo o evitarlo.

Se diseñarán unos controles de seguridad en función de la evaluación de riesgos, adoptando medidas técnicas, procesos operativos o políticas de seguridad. Centrándonos en los datos de nuestros clientes podremos optar por el cifrado, control de accesos y procedimientos en la gestión de datos.

Este enfoque basado en el riesgo no será algo estático, deberá plantearse como un proceso continuo, monitorizando, revisando regularmente los riesgos y los controles que hubiéramos implementado siendo un beneficio que nos aportará una constante adaptación a los cambios en las amenazas y vulnerabilidades.

La implementación de la ISO 27001 sigue un enfoque basado en el ciclo PDCA (Planificar, Hacer Verificar, Actuar) la cual es una metodología de mejora continua. Este ciclo se repite para garantizar la eficacia y mejora constante del Sistema de Gestión de Seguridad de la Información (SGSI).

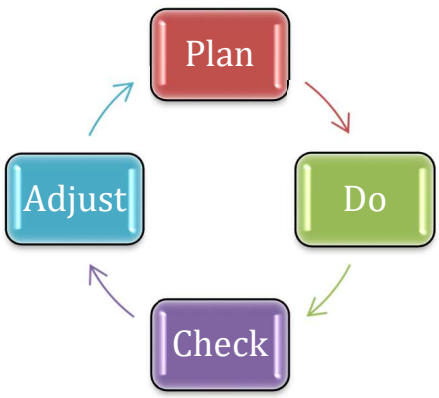

Ilustración 2. Ciclo PDCA. Fuente: Propia

La implementación de seguridad de la información de la ISO 27001 se compone de cláusulas aplicables a cualquier proyecto relacionado con seguridad de la información. El plan es la parte más importante porque es la base en la que se sustenta el desarrollo de un proyecto o hacer "Do" para finalmente pasar a la revisión "Check" y por último los ajustes o actuaciones "Adjust/Act" en caso necesario. A continuación se mostrará un cuadro con las cláusulas que aplicaremos y explicaremos brevemente su implementación en nuestro proyecto.

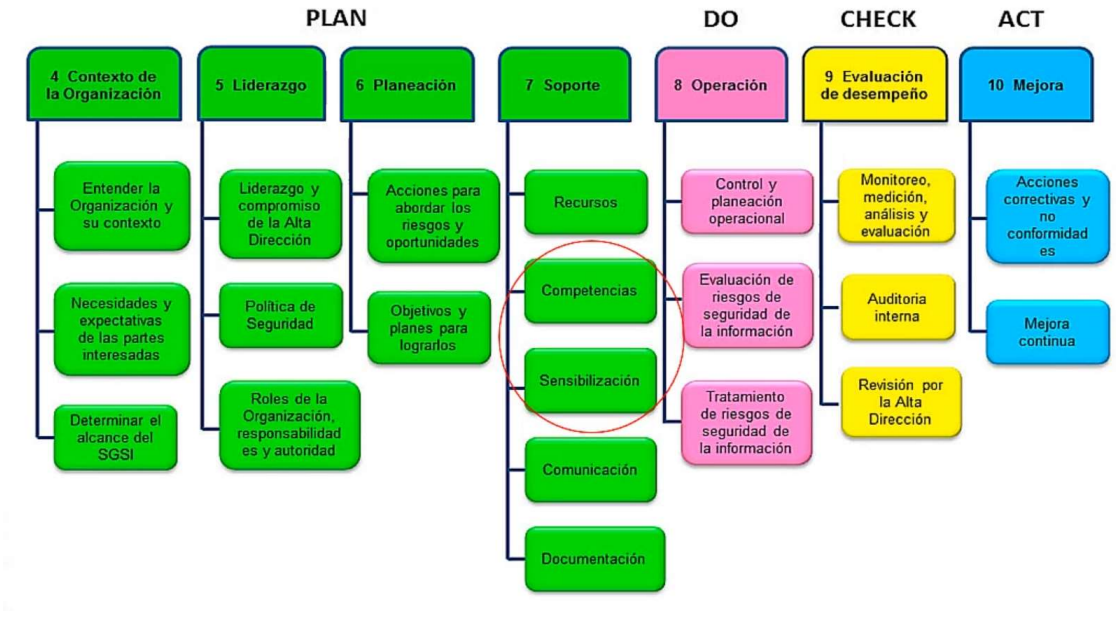

Ilustración 3. Cuadro PDCE. Fuente: udemy.es

6.2. Cláusulas de Implementación de la ISO 27001

PLAN

Clausula 4. **Contexto de la organización:** En el apartado 3.1 de antecedentes, se ha contextualizado la organización sobre la que se ha planificado el proyecto objeto del trabajo.

4.1. Entender la organización y su contexto: Se trata de una consultoría legal con una plantilla de 59 personas, tal y como se expresa en el plano de la organización, sin contar los laterales de la mesa de reuniones. Aunque sí se ha tenido en cuenta que aproximadamente 38 personas trabajan de manera remota, por lo que justifica el motivo de la disposición de una VPN.

4.2. Necesidades y expectativas de las partes interesadas: Se mantuvo una reunión con los miembros del departamento de dirección para para proceder a planificar un proyecto ajustado a las necesidades de los interesados e implementado de acuerdo a sus expectativas.

4.3. Determinar el alcance del SGSI: Identificando el tipo de datos confidenciales que maneja la empresa; información financiera, datos personales tanto de los empleados como de los clientes, contratos y acuerdos y documentación legal sensible, hace que los sistemas de información críticos sean fundamentales para el funcionamiento seguro de la empresa tanto

en las instalaciones físicas como para los empleados remotos, y dado que planteamos implementar VLANs por departamentos, se identifican y clasifican por actividad específica de cada departamento y la información asociada.

Clausula 5. Liderazgo: Es importante abordar esta cláusula de manera efectiva para que todo el personal adquiera el compromiso de seguridad con la nueva infraestructura desde la Alta Dirección.

5.1. Liderazgo y compromiso de la Alta Dirección: El departamento directivo se compromete activamente con la seguridad de la información, reconociendo su importancia estratégica para el éxito del proyecto.

5.2. Política de Seguridad: Se establecen unas política de seguridad de la información que mostraran el compromiso de la organización en referencia a la infraestructura de red y la información que se maneja. Las políticas serán claras y comprensibles para todos los miembros de la empresa, siendo adaptadas a cada rol, si fuese necesario.

5.3. Roles de la Organización, responsabilidades y autoridad: Esto se define y documenta, de acuerdo al puesto y responsabilidades relacionadas con la seguridad de la información en el contexto del proyecto de infraestructura de red. Debiéndose asignar distintos roles de la infraestructura de red:

- Un Jefe de Seguridad de la Información o también conocido como CISO: Será el Jefe responsable de toda la infraestructura de la red y seguridad de la información de la empresa.
- Un Responsable del Sistema de la Información (RSI): Será el responsable de todo el sistema, es decir, los dispositivos en los que se maneje información de la empresa.
- Un Administrador del Sistema (AS): Será el encargado de configurar la parte lógica del sistema.
- Usuarios del sistema: Son todos los usuarios de la empresa.

Cada uno de estos roles, están recogidos en las Políticas de Seguridad, y asimismo, se les asignan permisos y privilegios desde el Directorio Activo del servidor de dominio.

Clausula 6. Planeación: Se identifican y evalúan los riesgos y oportunidades relacionados con la seguridad de la información en el proyecto de infraestructura de red.

6.1. Acciones para abordar los riesgos y oportunidades: Se realiza una evaluación de riesgos que identifique las amenazas y vulnerabilidades específicas para desarrollar un plan de tratamiento de riesgos que incluya medidas preventivas y de mitigación.

6.2. Objetivos y planes para lograrlos: Los objetivos que se establecen están alineados con los objetivos del proyecto y la estrategia de la empresa. Por tanto, todo el plan de acción se desarrollará bajo las cláusulas anteriores acordadas con la Alta Dirección.

Clausula 7. Soporte:

7.1. Recursos: Se asignan los recursos necesarios para implementar y mantener las medidas de seguridad, asegurando la disponibilidad de los recursos financieros, humanos y tecnológicos, mientras se verifica que se cuenta con herramientas y tecnología que respalden la seguridad de la información.

7.2. Competencias: El personal que participa en el proyecto tiene la competencia necesaria para gestionar la seguridad de la información de manera efectiva. Por lo que se le proporcionará formación continua para mantener y mejorar las habilidades y conocimiento relacionados con la seguridad de la información, asegurando que el personal sea competente para abordar riesgos específicos del entorno de la infraestructura de red.

7.3. Sensibilización: Los programas de concienciación adaptados para todo el personal de la empresa para cada uno de los roles desempeñados en la empresa es imprescindible para prevenir las amenazas y asegurar las buenas prácticas.

7.4. Comunicación: Se debe establecer un proceso de comunicación efectivo para abordar asuntos relacionados con la seguridad, siendo canales claros para la comunicación interna y externa. Garantizando que sea oportuna y comprensible para todos.

7.5. Documentación: Será completa, actualizada y disponible para el personal relevante en el proyecto.

HACER "DO"

Clausula 8. Operación

8.1. Control y planeamiento operacional: A través del desarrollo y documentación de procedimientos operativos para la gestión de seguridad de la información e integración de medidas de seguridad en las operaciones diarias.

8.2. Evaluación de riesgos de seguridad de la información: Se realizan evaluaciones periódicas de riesgos para identificar nuevas amenazas y vulnerabilidades, ajustadas a las medidas de seguridad según sea necesario en función de los resultados de la evaluación de riesgos.

8.3. Tratamiento de riesgos de seguridad de la información: Hay riesgos que se aceptan como residuales, se transfieren, se mitigan o eliminan de manera documentada para poder desarrollar estrategias claras que aborden estos riesgos mediante implementación de controles adicionales o aceptación consciente o transferencia.

REVISAR "CHECK"

Clausula 9. Evaluación de desempeño

9.1. Monitoreo, medición, análisis y evaluación: Mediante la implementación de indicadores claves de rendimiento (KPIs)[3] relevantes para evaluar la eficacia del SGSI y estableciendo métodos para monitorear la implementación de controles y la gestión de riesgos.

9.2. Auditoría interna: Estas auditorías se realizan de forma periódica para asegurar que el plan de seguridad se implementa de acuerdo a las políticas establecidas y a las cláusulas de la ISO 27001. Estas auditorías deben ser imparciales y conducidas por personal competente.

9.3. Revisión por la alta dirección: La alta dirección revisa periódicamente el desempeño del SGSI en el proyecto para asegurar su idoneidad, adecuación y eficacia continua. La Alta Dirección programará revisiones para abordar los resultados de auditorías, el estado de los riesgos y la implementación de acciones correctivas y preventivas, asegurándose la mejora continua.

AJUSTAR "ADJUST"

Clausula 10. Mejora: Desarrollar y optimizar la infraestructura de red.

10.1. Acciones correctivas y no conformidades: Las acciones correctivas implementadas deben documentarse, así como los mecanismos, auditorías internas, revisiones de la dirección y reportes de incidentes para detectar no conformidades.

10.2. Mejora continua: Esta cláusula es fundamental y se fomenta en todos los niveles del SGSI del proyecto mediante una cultura organizacional que valore y priorice la mejora.

6.3. Infraestructura de Red y Seguridad

Nuestra propuesta es una estructura de red segura con direccionamiento fijo privado, firewall Palo Alto, switches, routers, servidor de dominio, servidor de archivos e impresión, SIEM, NAS y consola. Además, la evaluación de la posible utilización de AWS para respaldar la infraestructura y ofrecer redundancia.

Los elementos que utilizaremos se ajustan a las necesidades de la empresa, dispositivos utilizados por los empleados y los que se utilizaran en la nueva infraestructura. El cableado que se empleará será UTP, y asimismo, segmentaremos la red en V**LAN s** para prevenir ataques de ransomware y asegurar la disponibilidad de la información, así como VPN para aquellos trabajares que accedan desde el exterior o un terminal propio a la red de la empresa. Por otro

[3] KPI, son las siglas de "*Key Performance Indicator*" en inglés, y se traduce al español como "Indicador Clave de Desempeño". Es una medida que cuantifica el rendimiento de una organización, un proyecto, un proceso o incluso un empleado, en relación con sus metas y objetivos. (Nirian, 2020)

lado, en lo que a recursos se refiere y gestión de roles, se realizará a través de las máquinas virtuales, creando tantas como sean necesarias y ampliándose en caso de ser necesario por parte de la empresa a través de VMware.

Como ya se puso apreciar en el plano de la empresa (Ilustración 1), hay una sala de reuniones que estará tecnológicamente Equipada con tecnología VoIP, pantalla conectada a interruptor versátil y capacidad para reuniones virtuales.

La empresa se adapta a las nuevas tendencias y modalidades de trabajo, por este motivo, no sólo ofrece la posibilidad de trabajo remoto o hibrido, sino también que sus empleados usen su propio dispositivo si así lo prefieren para el desarrollo de sus actividades profesionales, adoptando las políticas pro-BYOD. Nuestro proyecte estará adaptado a las peticiones de nuestro cliente.

Por todo lo anteriormente dicho, nuestro modelo de infraestructura implementará medidas contra DDoS para proteger la disponibilidad de los servicios. Aunque no forma parte del desarrollo de nuestro proyecto, aconsejamos a nuestro cliente que contemple la posibilidad de instalar cámaras de seguridad y un acceso a la empresa y, especialmente al CPD a través de un dispositivo biométrico.

6.4. Segmentación de red, dispositivos y material

Para el direccionamiento IP utilizaremos el rango de direccionamiento 192.168.1.0/24. Este rango se segmenta y organizamos la red para brindar más seguridad, administración y rendimiento. Por tanto, asignaremos VLANs de la siguiente manera:

- **VLAN 10: Servidores**
  - Puertos de red: 6
  - Rango de direcciones IP: 192.168.1.1 - 192.168.1.8
  - Máscara de subred: 255.255.255.248(/28)
  - Dispositivos:
    - Router 1: 192.168.1.1
    - Router 2: 192.168.1.2
    - Firewall: 192.168.1.3
    - Servidor 1: 192.168.1.4
    - Servidor 2: 192.168.1.5
    - NAS: 192.168.1.6
    - Switch 1: 192.168.1.7
    - Switch 2: 192.168.1.8

- **VLAN 20: Administración**
  - Puertos de red: 4
  - Rango de direcciones IP: 192.168.1.9 - 192.168.1.12
  - Máscara de subred: 255.255.255.252(/30)

- **VLAN 30: Departamento Jurídico**
  - Puertos de red: 24
  - Rango de direcciones IP: 192.168.1.13 - 192.168.1.36
  - Máscara de subred: 255.255.255.224(/27)

- **VLAN 40: Directivos**
  - Puertos de red: 5
  - Rango de direcciones IP: 192.168.1.37 - 192.168.1.41
  - Máscara de subred: 255.255.255.248(/29)
- **VLAN 50: Sala de reuniones**
  - Puertos de red: 2
  - Rango de direcciones IP: 192.168.1.42 - 192.168.1.43
  - Máscara de subred: 255.255.255.252(/30)

- **VLAN 60: VoIP**
  - Puertos de red: 33
  - Rango de direcciones IP: 192.168.1.44 - 192.168.1.176
  - Máscara de subred: 255.255.255.192(/26)

Esto permitirá asignar diferentes rangos de direcciones IP a cada VLAN, proporcionando una separación lógica de las redes. Además, aplicaremos las políticas de seguridad específicas a cada VLAN según las necesidades de cada área.

Nos aseguraremos que nuestra infraestructura cuente con los switches y routers que admiten la configuración y manejos de las VLANs. También tendremos en cuenta la configuración adecuada del servidor de DHCP "*Dynamic Host Configuration Protocol*" (para las VLAN con IP automáticas.

Ilustración 4. Capas del modelo OSI. Fuente: prored.es

La selección de dispositivos electrónicos en el contexto del modelo de referencia OSI (Open Systems Interconnection) que trabajaremos serán los siguientes:

- **Switches Cisco Catalyst 2960-Plus 48PST-S:** a pesar de tener un costo inicial más alto que otras marcas, lo cierto es que ofrece confiabilidad y escalabilidad. Por lo que, a largo plazo podría ofrecernos más beneficios para una empresa en crecimiento. Utilizaremos dos switches con 48 puertos Fast Ethernet, en base a la cantidad de empleados en planta y la cantidad de nuestros dispositivos, tanto electrónicos, como VoIP y futuras expansiones.

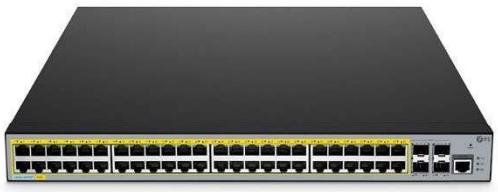

Ilustración 5. Switch Cisco Catalyst 2960-Plus 48PST-S. Fuente: cisco.com

- **Routers Cisco ISR 4000:** este modelo nos ofrece capacidades avanzadas de enrutamiento y soporte de configuración de VLANs. Teniendo en cuenta que debemos facilitar la interconexión entre las VLANs, y además, gestionar la conectividad externa, como la conexión a Internet, necesitaremos al menos dos routers.

Ahora bien, la integración de routers de la serie Integrated Services Router (ISR) de Cisco, como el ISR 4000 Series, con switches Catalyst, especialmente la serie Catalyst 2960, ofrece una sinergia excepcional para la infraestructura de red de una empresa. Esta compatibilidad proporciona una interoperabilidad sin fisuras, simplificando la configuración y gestión de la

red. Al utilizar dispositivos de la misma marca, la configuración se unifica, facilitando tareas de administración como la implementación de políticas de calidad de servicio (QoS)[4] y la gestión centralizada a través de herramientas como Cisco Prime Infrastructure. La seguridad también se beneficia al aplicar políticas coherentes en toda la infraestructura.

A largo plazo, esta elección brinda a la empresa una base escalable, permitiendo la expansión sin problemas a medida que crece. La confianza en la marca Cisco, respaldada por su reputación de confiabilidad y rendimiento, asegura una inversión duradera. Además, el soporte continuo y las actualizaciones de firmware proporcionados por Cisco garantizan que la infraestructura permanezca actualizada y protegida contra vulnerabilidades de seguridad. La integración con otras soluciones Cisco, si es relevante, proporciona una experiencia más cohesionada. En resumen, la elección de routers ISR junto con switches Catalyst no solo ofrece beneficios inmediatos en términos de compatibilidad y gestión simplificada, sino que también establece una base sólida y confiable para el crecimiento y desarrollo continuo de la empresa.

Ilustración 6. Router Cisco IRS 4000. Fuente: cisco.com

- **Firewall Palo Alto Networks PA-820:** después de una exhaustiva búsqueda, nos hemos decantado por este dispositivo por ser una opción robusta con el que podremos configurar las reglas de configuración de tráfico, considerando las políticas de filtrado, inspección profunda, de paquetes y prevención de intrusiones. En nuestro caso, precisamos de un solo firewall, aunque quizás estés pensando en la VPN, pero hemos decidido que conlleva muchas más ventajas una externa, más adelante explicaremos los motivos en el apartado VPN. Además, nuestro firewall es compatible con nuestros switches y routers, aunque esto no resulta muy difícil porque tanto los switches, como los routers y el firewall son dispositivos de red y, por tanto, operan en diferentes capas del modelo OSI (ver figura 4). Para esta infraestructura hemos tenido en cuenta lo siguiente:

    - Configuraciones de VLANs para garantizar la segmentación de red y seguridad adecuada.
    - Enrutamiento e interconexión para permitir el tráfico entre las VLANs hacia y desde el firewall.
    - Seguridad y Políticas para controlar el tráfico entre las diferentes partes de la red.

[4] QoS son las siglas en inglés de "*Quality of Service*", en español "Calidad de Servicio". Es un conjunto de tecnologías y mecanismos diseñados para gestionar y mejorar la calidad de los servicios de red, especialmente en entornos donde la fiabilidad y el rendimiento son críticos. (Techtarget, 2021)

Ilustración 7. Firewall Palo Alto Networks PA-820. Fuente: paloaltonetworks.com

- **Servidores**: hemos decidido utilizar dos servidores físicos en modo espejo con Windows Server 2022 en clúster de alta disponibilidad y servidores virtuales para el controlador de dominio, servidor de archivos e impresión, y SIEM. Está configuración nos va a garantizar la continuidad operativa y la recuperación de desastres.

Tras una valoración en el mercado entre los distintos fabricantes de servidores y teniendo en cuenta que para nuestro cliente es más importante un alto rendimiento, escalabilidad, la seguridad y servicio. Este momento ha sido crucial, pero nuestra experiencia nos ha dicho que consideraríamos una **arquitectura hiperconvergente** porque no sólo integrará servidores, almacenamiento y redes, sino también virtualización directamente en el sistema. De esta manera, tendremos un sistema más escalable de manera granular y sencilla, más flexible al agregar módulos individuales según sea necesario y una gestión más simplificada mediante el uso de un panel de control para administrar los recursos. Por otra parte, las máquinas virtuales nos van a permitir una mayor flexibilidad y gestión eficiente de recursos, mediante asignación de IP dentro del rango de la VLAN 10 para cada máquina virtual.

Servidores Físicos:

- dos HPE ProLiant DL380 Gen10
- un Synology RackStation RS3618xs.

El servidor HPE ProLiant DL380 Gen10 ofrece opciones de configuración con potentes procesadores, capacidad de memoria escalable y opciones de almacenamiento que se adaptan a entornos virtualizados. Además, brinda una buena gestión en eficiencia energética. Aunque tiene un precio más alto que sus competidores DELL y Supermicro, su calidad y escalabilidad merecen la pena. En cuanto a la parte lógica de nuestra infraestructura, necesitaremos dos direcciones IP fijas para la configuración del clúster (una para cada servidor) y una dirección IP virtual que se moverá entre los servidores en caso de conmutación por error.

Especificaciones técnicas HPE ProLiant DL380 Gen10:

- PROCESADOR: Intel Xeon
- RAM: 16 Gb
- ROM: 128 GB una unidad SDD

Ilustración 8. Servidor HPE Proliant DL380 Gen 10. Fuente: nuy.hpe.com

El servidor NAS podría ser físico o virtual, pero para este proyecto hemos optado por uno físico, el Synology RackStation RS3618xs, con velocidades de red Gigabit para garantizar un rendimiento adecuado, en cuanto a la gestión de grandes volúmenes de información y acceso rápido, capacidad de ampliación de unidades de almacenamiento o discos duros adicionales. Además, utilizaremos la tecnología RAID 10 que nos proporciona mayor redundancia y rendimiento. El servidor estará dentro de la VLAN 10 de servidores para obtener el más alto rendimiento y baja latencia entre sí.

Especificaciones técnicas Synology RackStation RS3618xs:

- PROCESADOR: Intel Xeon D-1521 de cuatro núcleos.
- RAM: 16 Gb
- Almacenamiento: 100 TB
- Sistema Operativo: Windows Server 2022

Ilustración 9. Servidor NAS Synology RackStation RS3618xs. Fuente: synology.com

Un Sistema de Alimentación Ininterrumpida (SAI) es un componente crucial para mantener la continuidad de energía en sistemas electrónicos ya que nos proporcionará respaldo de energía en caso de cortes eléctricos.

Tendremos en cuenta la capacidad total de carga, la duración de respaldo. Por ello nos decantamos por la marca ACP y el modelo Smart-UPS.

La suma de la carga en vatios (W) de todos los dispositivos que colocaremos en el armario nos hará decantarnos por ese modelo y la capacidad de esta será suficiente para manejar esta carga.

Ilustración 10. Sistema de Alimentación Ininterrumpida ACP Smart-UPS. Fuente: acp-com

- **Armario Rack. Características y distribución.**

Para alojar todos los equipos necesarios de nuestra infraestructura se ha elegido en el armario de marca El Tripp Lite SR42UBCL por su versatilidad y capacidad. Adaptado para almacenar nuestro dispositivos y con la suficiente refrigeración. Además la CPD tendrá un sistema de climatización automático, manteniendo la sala a una temperatura constante de 16º, teniendo un sistema de aviso por sonido en caso de subir su temperatura.

El tamaño del armario es estándar de 42 unidades de rack (42U) proporciona un espacio significativo para albergar múltiples servidores y equipos de red en un solo armario. Cuenta con un ventilador superior para mantener una temperatura adecuada dentro del armario, y así evitar el sobrecalentamiento de los equipos. Esto es especialmente importante en entornos donde se utilizan servidores y equipos de red de alta densidad.

Las puertas perforadas permiten la circulación del aire, facilitando la refrigeración natural y ayudando a mantener una temperatura ideal en el interior del armario.

El diseño del armario está pensado para ser compatible con equipos Cisco, asegurando que los servidores y otros dispositivos puedan montar y funcionar eficientemente dentro del armario.

Ilustración 11. Armario El Tripp Lite SR42UBCL. Fuente: amazon.com

La gestión de cables integrada es esencial para mantener un entorno organizado y facilitar el acceso a los componentes cuando sea necesario por lo que un buen sistema de gestión de cables nos ayudará a reducir el desorden y a simplificar la administración del armario.

Estas características hacen que el armario elegido sea una opción sólida para nosotros que buscamos un armario de servidor compatible con diferentes equipos y que ofrezca un entorno bien refrigerado y organizado.

Considerando la seguridad física del rack, se ha colocado el CPD en el lugar más seguro de la empresa y utilizaremos cerraduras en las puertas del rack para evitar el acceso no autorizado.

Comenzando el montaje de todos los dispositivos en el rack, seguiremos ciertos principios para optimizar la organización y el rendimiento de nuestra infraestructura de red. Los dispositivos comprados van desde las dos alturas como los switches hasta los routers que ocupan seis.

Utilizaremos bandejas para organizar el cableado, asegurándonos la correcta etiquetación para facilitar el mantenimiento y la resolución de futuros problemas. Con abrazaderas mantendremos los cables ordenados evitando enredos que dificulten el trabajo. Se planificará cuidadosamente el enrutamiento de cables para asegurar una buena circulación de aire para la refrigeración, para ello utilizaremos guías y paneles de parcheo.

Para las conexiones entre dispositivos que utilizan cableado Ethernet, tendremos en cuenta la longitud del cableado, que se adecuada evitando tener que hacer cocas y futuros fallos de conexión.

Documentamos todo el proceso de montaje y cualquier otra información relevante para facilitar futuras actualizaciones y resoluciones de problemas ya que creemos que la organización y la documentación son clave para mantener una red eficiente y fácil de administrar.

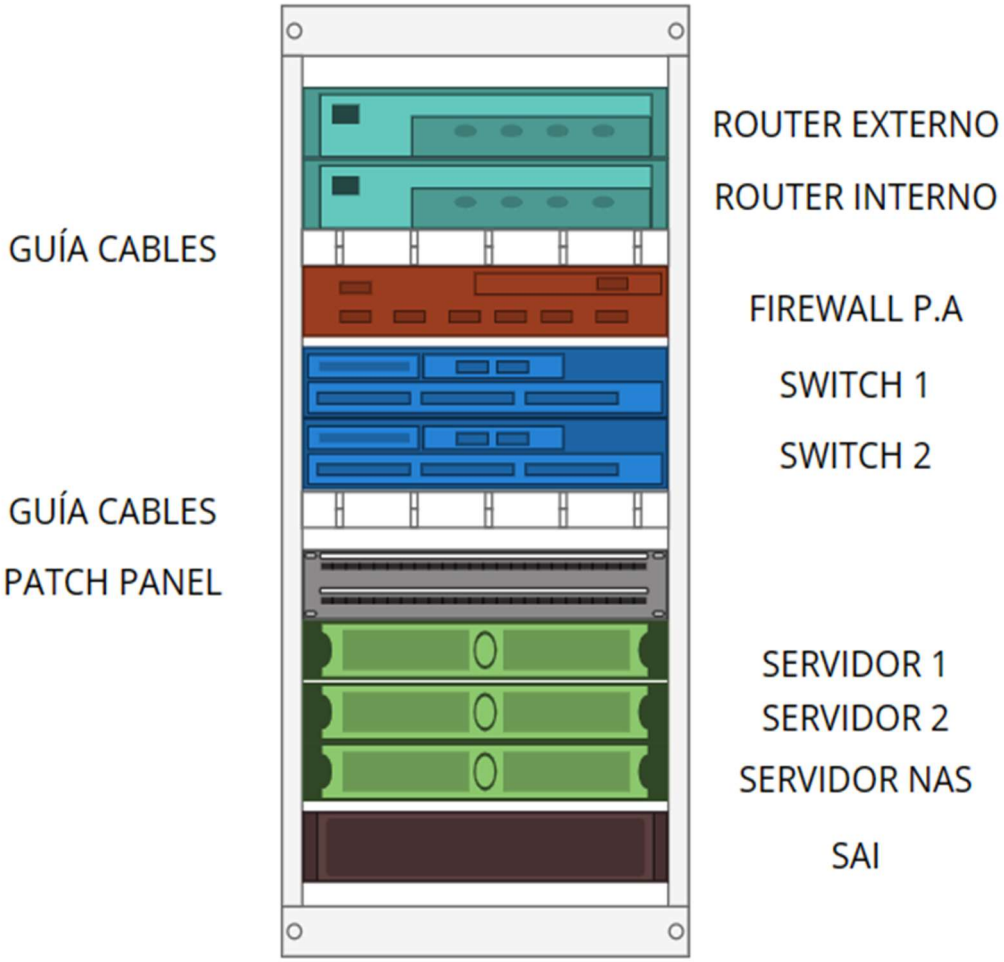

Ilustración 12. Distribución del armario. Fuente: Propia.

Los cables Ethernet se utilizan para conectar dispositivos de red entre sí, y pueden ser de dos tipos principales: cables directos y cables cruzados. La diferencia entre ellos radica en cómo se conectan los pares de cables dentro del conector RJ45 (el conector estándar para cables

Ethernet). A continuación, explicaremos la diferencia entre cable Ethernet Directo y cable Ethernet Cruzado.

- **Cable Ethernet Directo:**

En un cable directo, los pines en un extremo del cable coinciden directamente con los pines en el otro extremo del cable.

Los cables directos se utilizan para conectar dispositivos que tienen funciones opuestas en una red, como un equipo a un switch o a un Router.

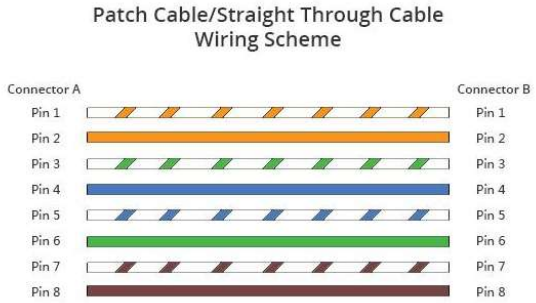

Ilustración 13. Código de colores directo. Fuente: community.fs.com

- **Cable Ethernet Cruzado:**

En un cable cruzado, los pines en un extremo del cable se cruzan o intercambian con los pines en el otro extremo del cable.

Los cables cruzados se utilizan para conectar dispositivos que tienen funciones similares en una red, como dos equipos, dos switches o dos enrutadores.

Es importante mencionar que en la actualidad muchos dispositivos de red modernos admiten la función de "Auto MDI-X" (Auto Crossover), que permite que un puerto se comporte como si estuviera conectado a un cable directo o cruzado, eliminando la necesidad de preocuparse por el tipo de cable que se está utilizando. Sin embargo, aún puede ser útil conocer la distinción entre cables directos y cruzados, especialmente al trabajar con hardware más antiguo.

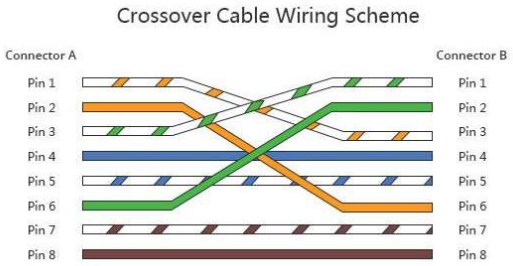

Ilustración 14. Código de colores cruzado. Fuente: community.fs.com

6.5. Configuración Router Externo

Configuraremos la interfaz que se conectará a internet WAN (*Wide Area Work*) con una conexión Ethernet.

```
interface GigabitEthernet0/0
  ip address 192.168.1.1 255.255.255.248
  description Conexión a Internet
  crypto map VPN_MAP
  no shutdown
exit
```

Ilustración 15. Consola Router Externo. Fuente: Propia

6.6. Configuración Router Interno

Configuraremos el Router accediendo a consola de administración. Deberemos asegurarnos que la configuración de las interfaces virtuales del Router coincida con las configuraciones de las VLANs en el Switch.

1º) Accederemos al modo configuración del Router:

```
Router> enable
Router# configure terminal
```

Ilustración 16. Consola Router Interno. Fuente: Propia

2º) Crearemos una interfaz/subinterfaz como se muestra en la Ilustración 17 siguiente:

```
Router(config)# interface GigabitEthernet0/1.10
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 10
Router(config-if)# ip address 192.168.1.1 255.255.255.248
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/7.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.1.7 255.255.255.252
Router(config-subif)# exit

Router(config)# interface GigabitEthernet0/11.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.1.11 255.255.255.224
Router(config-subif)# exit

Router(config)# interface GigabitEthernet0/35.40
Router(config-subif)# encapsulation dot1Q 40
Router(config-subif)# ip address 192.168.1.35 255.255.255.248
Router(config-subif)# exit

Router(config)# interface GigabitEthernet0/40.50
Router(config-subif)# encapsulation dot1Q 50
Router(config-subif)# ip address 192.168.1.40 255.255.255.252
Router(config-subif)# exit

Router(config)# interface GigabitEthernet0/44.60
Router(config-subif)# encapsulation dot1Q 60
Router(config-subif)# ip address 192.168.1.144 255.255.255.192
Router(config-subif)# exit
```

Ilustración 17. Consola Router Interno. Fuente: Propia

3º) Crearemos listas de control de acceso o conocido por siglas en inglés "*ACL*" para denegar el tráfico entre las VLANs bloqueando el tráfico entre las direcciones IP de las subredes de las VLANs.

```
Router(config)# access-list 100 deny ip 192.168.1.1 0.0.0.7 192.168.1.7 0.0.0.3
Router(config)# access-list 100 deny ip 192.168.1.1 0.0.0.7 192.168.1.11 0.0.0.31
Router(config)# access-list 100 deny ip 192.168.1.1 0.0.0.7 192.168.1.35 0.0.0.7
Router(config)# access-list 100 deny ip 192.168.1.1 0.0.0.7 192.168.1.40 0.0.0.3
Router(config)# access-list 100 deny ip 192.168.1.1 0.0.0.7 192.168.1.44 0.0.0.63

Router(config)# access-list 100 deny ip 192.168.1.7 0.0.0.3 192.168.1.11 0.0.0.31
Router(config)# access-list 100 deny ip 192.168.1.7 0.0.0.3 192.168.1.35 0.0.0.7
Router(config)# access-list 100 deny ip 192.168.1.7 0.0.0.3 192.168.1.40 0.0.0.3
Router(config)# access-list 100 deny ip 192.168.1.7 0.0.0.3 192.168.1.44 0.0.0.63

Router(config)# access-list 100 deny ip 192.168.1.11 0.0.0.31 192.168.1.35 0.0.0.7
Router(config)# access-list 100 deny ip 192.168.1.11 0.0.0.31 192.168.1.40 0.0.0.3
Router(config)# access-list 100 deny ip 192.168.1.11 0.0.0.31 192.168.1.44 0.0.0.63

Router(config)# access-list 100 deny ip 192.168.1.35 0.0.0.7 192.168.1.40 0.0.0.3
Router(config)# access-list 100 deny ip 192.168.1.35 0.0.0.7 192.168.1.44 0.0.0.63

Router(config)# access-list 100 deny ip 192.168.1.40 0.0.0.3 192.168.1.44 0.0.0.63

Router(config)# access-list 100 permit ip any any
```

Ilustración 18. Consola Router Interno. Fuente: Propia

4º) Configuraremos las rutas estáticas, como se muestra a continuación:

```
Router(config)# ip route 192.168.1.1 255.255.255.0 192.168.1.6
```

Ilustración 19. Consola Router Interno. Fuente: Propia

5º) Accederemos en modo de verificación y guardaremos la configuración:

```
Router# show interfaces
Router# show ip route


Router# write memory
```

Ilustración 20. Consola Router. Fuente: Propia

6.7. Configuración del Firewall Palo Alto

Configurar el firewall, como en el caso de Palo Alto, es un paso crucial para garantizar la seguridad de la infraestructura de red a implementar.

En un entorno donde vamos a utilizar VLANs para segmentar por departamentos en lo switches y al querer implementar un firewall Palo Alto, deberemos realizar varias configuraciones que habrá que tener en cuenta asegurar la conectividad segura entre las VLANs y proporcionar una capa adicional de seguridad.

1º) Configuración de Interfaz: La configuración de interfaces en un firewall, implica asignar interfaces físicas a las VLANs específicas como ya hemos descrito anteriormente y ahora configuramos.

```
# Configuración de la interfaz para Switch 1 - VLAN 10

set interface ethernet1/1
set zone "Switch1_VLAN_10"
set virtual-wire
set virtual-wire ingress-interface ethernet1/1
set virtual-wire egress-interface ethernet1/1
set interface ethernet1/1.10 tag 10
set interface ethernet1/1.10 ip 192.168.1.1/29

# Configuración de la interfaz para Switch 1 - VLAN 20
set interface ethernet1/1.20 tag 20
set interface ethernet1/1.20 ip 192.168.1.7/30

# Configuración de la interfaz para Switch 1 - VLAN 30
set interface ethernet1/1.30 tag 30
set interface ethernet1/1.30 ip 192.168.1.11/27

# Configuración de la interfaz para Switch 1 - VLAN 40
set interface ethernet1/1.40 tag 40
set interface ethernet1/1.40 ip 192.168.1.35/29

# Configuración de la interfaz para Switch 1 - VLAN 50
set interface ethernet1/1.50 tag 50
set interface ethernet1/1.50 ip 192.168.1.40/30




# Configuración de la interfaz para Switch 2 - VLAN 60
set interface ethernet1/2
set zone "Switch2_VLAN_60"
set virtual-wire
set virtual-wire ingress-interface ethernet1/2
set virtual-wire egress-interface ethernet1/2
set interface ethernet1/2.60 tag 30
set interface ethernet1/2.60 ip 192.168.31.44/26



# Aplicar configuraciones
commit
save config
```

Ilustración 21. Consola Firewall. Configuración de Interfaz Fuente: Propia

2º) Configuración de las Zonas: Asignamos las interfaces a las zonas correspondientes.

```
# Switch 1 - VLAN 10
set zone "Servidores_Zone"
set interface ethernet1/1.10
exit

# Switch 1 - VLAN 20
set zone "Administracion_Zone"
set interface ethernet1/2.20
exit

# Switch 1 - VLAN 30
set zone "Juridico_Zone"
set interface ethernet1/3.30
exit

# Switch 1 - VLAN 40
set zone "Directivos_Zone"
set interface ethernet1/4.40
exit

# Switch 1 - VLAN 50
set zone "Sala_reuniones_Zone"
set interface ethernet1/5.50
exit


# Switch 2 - VLAN 60
set zone "VOIP_Zone"
set interface ethernet1/1.60
exit



# Aplicar configuraciones
commit
save config
```

Ilustración 22. Consola Firewall. Configuración de las Zonas Fuente: Propia

6.8. Configuración Switch 1

Una vez cableados los dispositivos, en la parte lógica, comenzaremos a crear las VLANs anteriormente definidas con la configuración, tanto del router, como del switch seguido del firewall mediante comandos. Todo ello desde la consola de cada dispositivo con el perfil de Administrador.

Al elegir modelos gestionables que admiten VLAN (IEEE 802.1.Q) con una interfaz de línea de comandos, accedemos a la parte de configuración del switch e introducimos los siguientes comandos:

1º) Acceso modo configuración del Switch:

```
switch> enable
switch# configure terminal
```

Ilustración 23. Consola Switch 1. Acceso modo configuración Fuente: Propia

2º) Creación VLAN:

```
switch(config)# vlan 10
switch(config-vlan)# name SERVIDORES
switch(config-vlan)# exit

switch(config)# vlan 20
switch(config-vlan)# name ADMINSTRACION
switch(config-vlan)# exit

switch(config)# vlan 30
switch(config-vlan)# name DEPARTAMENTO JURIDICO
switch(config-vlan)# exit

switch(config)# vlan 40
switch(config-vlan)# DIRECTIVOS
switch(config-vlan)# exit

switch(config)# vlan 50
switch(config-vlan)# SALA DE REUNIONES
switch(config-vlan)# exit
```

Ilustración 24. Consola Switch 1. Creación de VLAN. Fuente: Propia

3º) Asignar puertos a las VLANs:

```
switch(config)# interface range fastEthernet 1/0/1 - 6
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 10
switch(config-if-range)# exit

switch(config)# interface range fastEthernet 1/0/7 - 10
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 20

switch(config-if-range)# exit
switch(config)# interface range fastEthernet 1/0/11 - 34
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 30
switch(config-if-range)# exit

switch(config)# interface range fastEthernet 1/0/35 - 39
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 40
switch(config-if-range)# exit
switch(config)# interface range fastEthernet 1/0/40 - 43
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 50
switch(config-if-range)# exit
```

Ilustración 25. Consola Switch 1. Asignación de Puertos VLAN Fuente: Propia

4º) Verificar y guardar la configuración:

```
switch# show vlan
switch# show interfaces status

switch# write memory
```

Ilustración 26. Consola Switch 1. Verificar y guardar. Fuente: Propia

6.9. Configuración Switch 2

1º) Acceso modo configuración del Switch:

```
switch> enable
switch# configure terminal
```

Ilustración 27. Consola Switch 2. Acceso modo configuración. Fuente: Propia

2º) Creación VLAN:

```
switch(config)# vlan 60
switch(config-vlan)# name VOIP
switch(config-vlan)# exit
```

Ilustración 28. Consola Switch 2. Creación VLAN. Fuente: Propia

3º) Asignar puertos a las VLANs:

```
switch(config)# interface range fastEthernet 1/0/44 - 179
switch(config-if-range)# switchport mode access
switch(config-if-range)# switchport access vlan 60
switch(config-if-range)# exit
```

Ilustración 29. Consola Switch 2. Asignar puertos a las VLAN. Fuente: Propia

4º) Verificar y guardar la configuración:

```
switch# show vlan
switch# show interfaces status

switch# write memory
```

Ilustración 30. Consola Switch 2. Verificar y guardar configuración. Fuente: Propia

6.10. Configuración del Clúster de los Servidores y NAS

Crear un clúster con dos servidores implica configurar una infraestructura que permita la distribución de la carga de trabajo, la alta disponibilidad y la tolerancia a fallos.

Requisitos previos

- Los dos servidores deberán tener hardware compatible.
- El servidor NAS elegido admite funciones de alta disponibilidad.
- Compatibles con el sistema operativo Windows Server 2022
- Hemos instalado las últimas actualizaciones de firmware y los controladores más recientes desde el sitio oficial de HPE.

Instalación de Windows Server 2022: Instalamos en la asignación de los 128GB el sistema operativo en ambos servidores mediante una imagen ISO y configuramos una unidad SDD para las aplicaciones.

- Configuración de la red:
    - Asignaremos direcciones estáticas a cada uno de los servidores físicos: servidor 1, servidor 2 y NAS.
    - Conectaremos ambos servidores 1 y 2 a una red para la comunicación entre ellos.

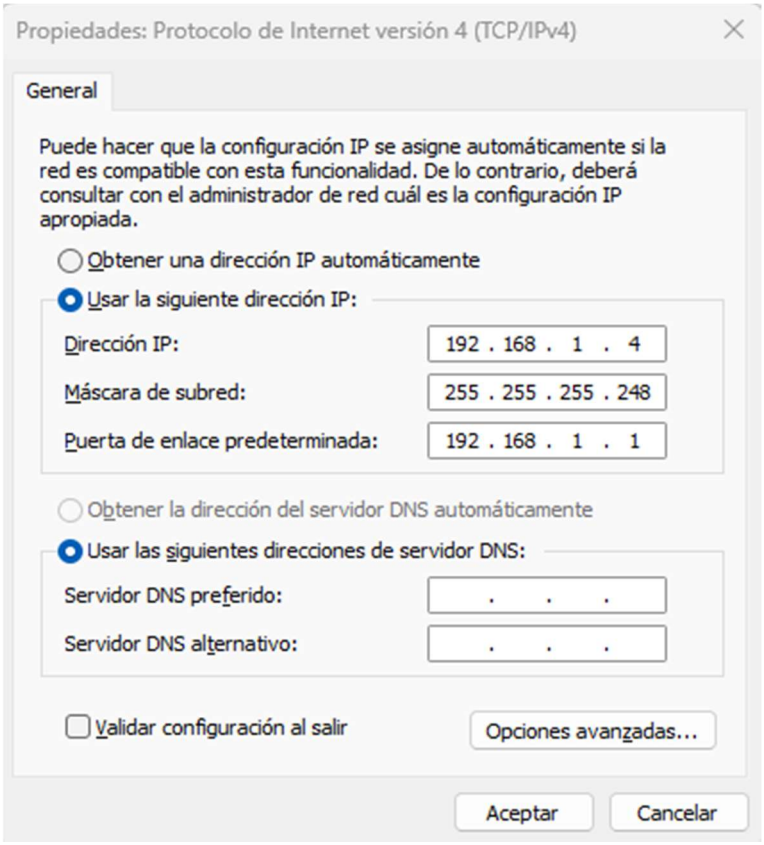

Ilustración 31. Asignar IP fija en servidor 1. Fuente: Propia

Configuración de almacenamiento:

- Hemos configurado la unidad SSD para las aplicaciones y nos hemos asegurado que están formateadas correctamente.
- Hemos utilizado la administración de discos de Windows para realizar cualquier configuración adicional.

Configuración del Clúster: Roles y conmutación por errores.

- Se abrió la herramienta "Administrador de clúster de conmutación por error"
- Se inició el asistente para configurar el nuevo clúster
- Se siguió las instrucciones para agregar ambos servidores al clúster.
- Se configuró la unidad SSD como un recurso compartido de clúster para las aplicaciones.
- Se configuró la conmutación por error para los roles y recursos críticos.

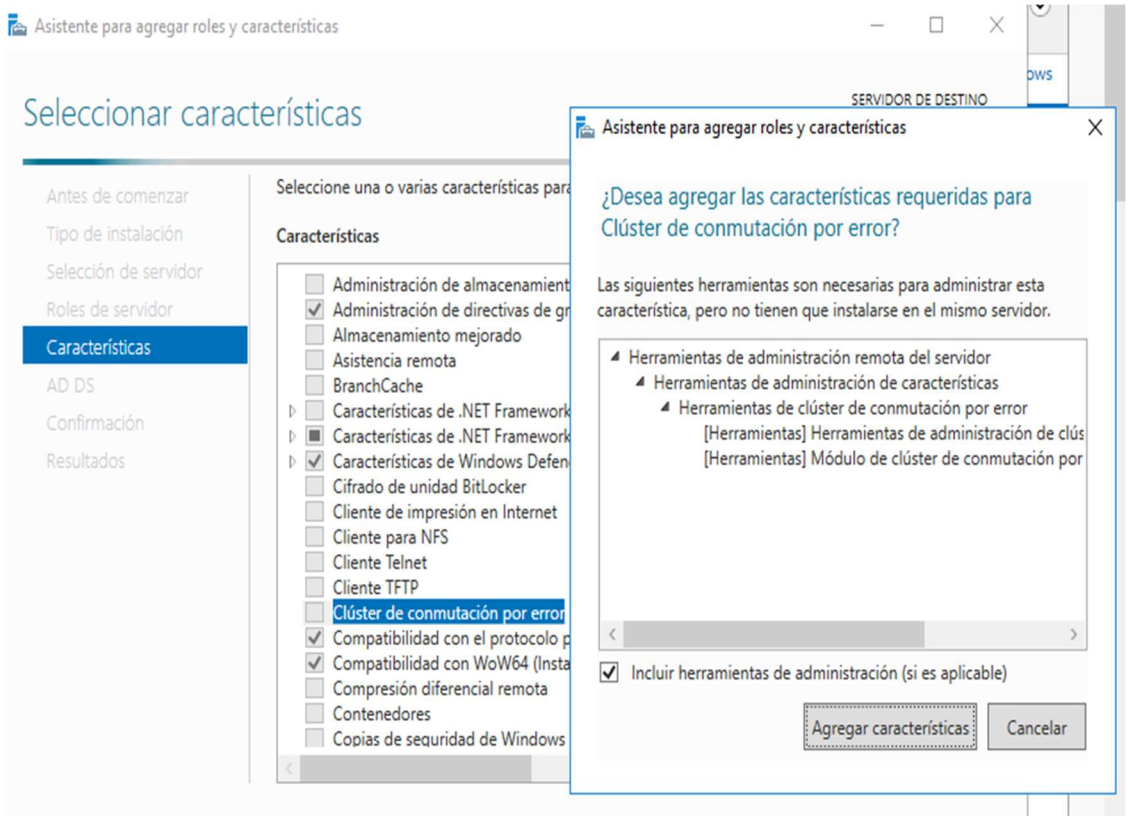

Ilustración 32. Agregar Clúster de conmutación por error. Fuente: Propia

Prueba de monitoreo: Se realizó prueba de conmutación por error para asegurarse que el clúster funcionaba correctamente y se configuró la monitorización para recibir alertas en caso de fallos o problemas.

Habilitación de replicación por DFS: Se ha considerado habilitar la Replicación por DFS, la cual permite replicar archivos y carpetas para garantizar la disponibilidad y redundancia de datos. La replicación ayudará a proporcionar una alta disponibilidad de los datos almacenados, mejorará la tolerancia a fallos al proporcionar copias redundantes de los archivos en diferentes ubicaciones. Por último, ayudará a distribuir la carga de la lectura entre los servidores.

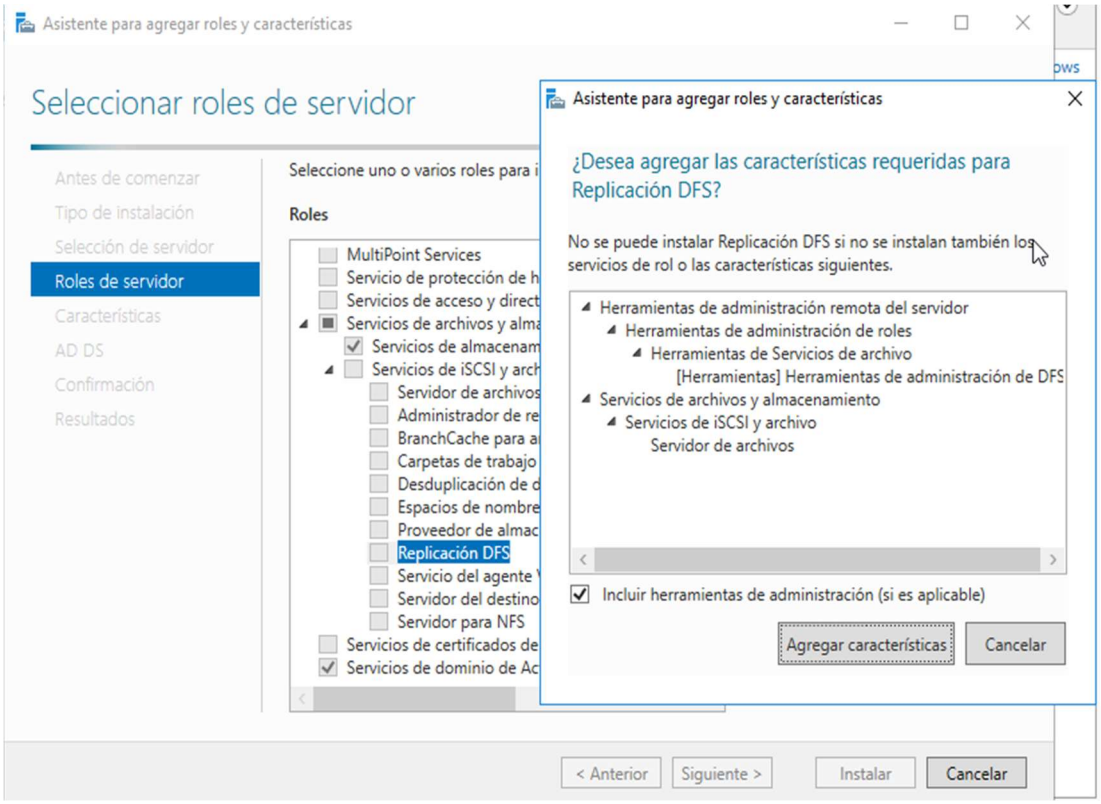

Ilustración 33. Replicación DFS. Fuente: Propia

6.11. UTP, VPN y virtualización

Dada nuestra infraestructura de red y seguridad, y teniendo en cuenta, que la empresa para la que estamos realizando el proyecto se encuentra en la planta de uno de los edificios de la Castellana en Madrid, el **UTP blindado (STP)** nos proporcionará mejor protección contra posibles Interferencias Electromagnéticas (EMI).

Tras reunirnos con el comité directivo de la empresa sobre sus necesidades en lo que se refiere al acceso remoto de sus empleados y terceros, hemos visto que la opción más ajustada es **AWS Site-to-Site VPN** porque nos ofrece una Infraestructura en la Nube segura y escalable, sin tener que gestionar una infraestructura física de una VPN propia. La nube nos permite ajustar los recursos de la red según las necesidades cambiantes del proyecto, siendo elástica a los cambios que puedan producirse en la carga de trabajo o requisitos de conectividad. Además, la implementación y configuración de la conexión VPN es sencilla e intuitiva, reduciendo en gran

medida la complejidad operativa. Este servicio ofrece una seguridad robusta alineada al cumplimiento normativo que necesitamos, contando con una alta resiliencia y disponibilidad para garantizar en todo momento la continuidad del trabajo, incluso en caso de fallos en los enlaces o centros de datos. También es interesante que los costos se optimicen en relación al uso real de los recursos por parte de la empresa, resultando más rentable de mantener y gestionar.

Como ya se reseñó en los objetivos, nuestra recomendación y mejor opción fue AWS Site-to-Site VPN por proporcionar conexiones seguras entre nuestra red local y la red Amazon VPC (Virtual Private Cloud) que es el servicio de red en la nube. La VPC nos permitirá crear secciones aisladas y lógicamente separadas en la nube y cada VPC será completamente independiente de las demás. Por lo que la empresa contará con su propia red privada en la nube, permitiéndonos controlar y personalizar la infraestructura de red para sus aplicaciones y servicios en AWS.

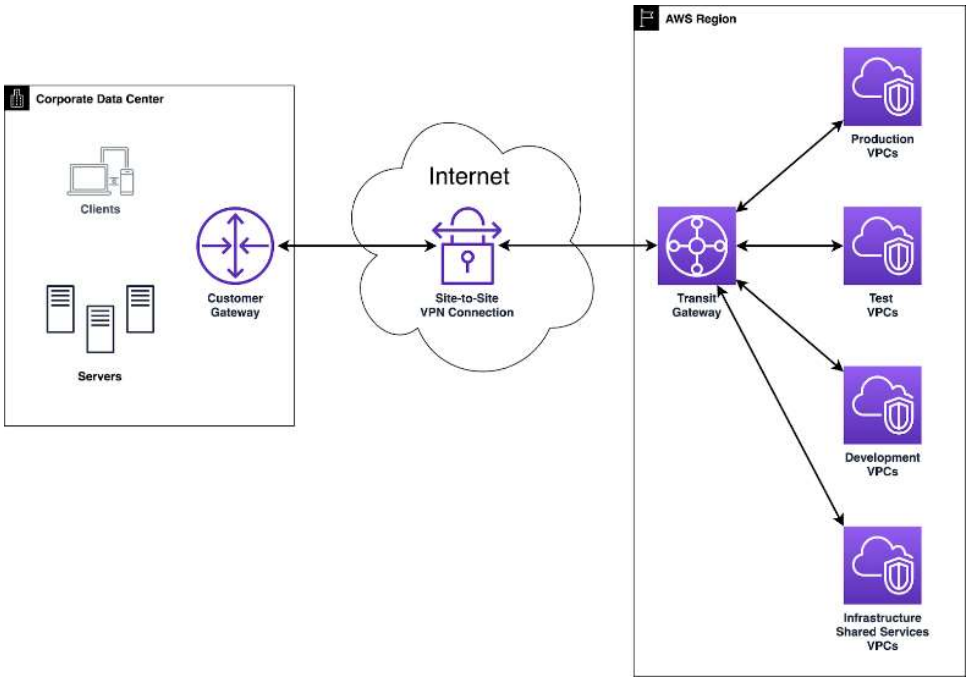

Ilustración 34. Arquitectura Site-to-Site VPN. Fuente: awsworkshop.io

A miles y miles de empresas tanto privadas como públicas les preocupa cómo mitigar o reducir los ataques de ransomware. Actualmente ha habido un caso mediático en el Ayuntamiento de Sevilla, incluso en Madrid el Alcalde Almeida, invierte mucho en este tipo de seguridad en sus Administraciones dependientes y que debemos tomar como ejemplo para el cuidado de nuestra empresa.

Para conseguir que nuestra empresa esté protegida de este ataque, deberemos implementar una combinación de medidas técnicas, prácticas de seguridad y concienciación del usuario.

Realizaremos copias de seguridad regularmente de los datos críticos, fuera de línea y en un lugar seguro. Esta práctica es esencial para la recuperación de datos en caso de ataque.

Tener el software actualizado, aplicando parches y actualizaciones de seguridad para el sistema operativo y todas las aplicaciones instaladas. Los fabricantes lanzarán actualizaciones para corregir vulnerabilidades conocidas y deberemos estar atentos a estas.

La instalación de un antivirus de un antimalware confiable, su correspondiente mantenimiento. Lo configuraremos para realizar escaneos automáticos y recibir actualizaciones de manera regular.

Implementaremos filtros de correo electrónico que bloqueen mensajes de phishing y correos electrónicos maliciosos. Importante la parte humana, educando al usuario para que desconfíe de enlaces y archivos adjuntos no solicitados.

Limitaremos los privilegios de usuario para que solo tengas acceso a los recursos y archivos necesarios para sus funciones, esto reducirá el impacto en caso de compromiso.

Monitorizamos la red y sistemas para detectar patrones de tráfico inusuales o comportamientos de archivos sospechosos.

Cifrar los datos sensibles para protegerlos, tanto en tránsito como en reposos. Esto reducirá la utilidad de los datos para los atacantes incluso si logran acceder a ellos.

Limitaremos y controlaremos los dispositivos extraíbles como unidades USB para prevenir la propagación de este ataque a través de medios externos.

Al adoptar un enfoque integral y proactivo, podremos mitigar significativamente el riesgo de ransomware y minimizar el impacto en caso de un incidente. La seguridad cibernética es un esfuerzo continuo, y la concienciación y preparación son la clave para la protección contra amenazas en constante evolución.

La virtualización de nuestras máquinas virtuales correrá en **VMware vSphere**, está siendo en servicio determinante para cualquier empresa que trabaje con recursos informáticos, nos proporcionará los recursos necesarios para la instalación y administración de la infraestructura con rendimiento y alta disponibilidad. Entre sus características más importantes encontraremos:

- Hypervisor ESXI
- vCenter Server (Gestiona la infraestructura)
- Almacenamiento compartido
- Funciones de alta disponibilidad (vMotion, HA, DRS, Fault Tolerance)

La instalación de este software la haremos en los servidores físicos, incluyendo **vMotion** para el controlador de dominio, el servidor de archivos e impresión y el servidor SIEM. Configuraremos el clúster de VMware para aprovechar al máximo la redundancia y la tolerancia a fallos e incluiremos vMotion para migración de máquinas virtuales entre servidores físicos en caso de problemas. Nuestros servidores físicos tendrán acceso al

almacenamiento compartido del NAS Synology, que es esencial para garantizar la migración entre los servidores clúster.

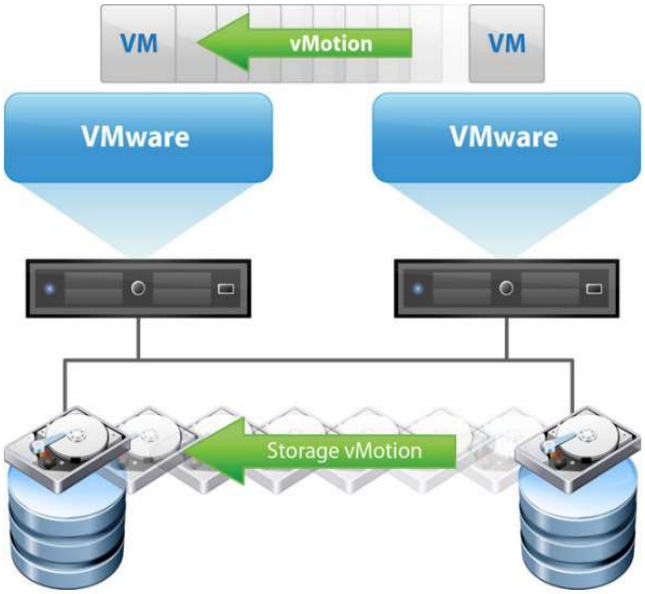

Ilustración 35. Arquitectura VMware con vMotion. Fuente: pluralsight.com

Nos queremos asegurar que contamos con las mejores prácticas de seguridad, por lo que implementaremos un protocolo de acceso seguro SMB 3.0 con encriptación, y así, aplicaremos medidas de seguridad adicionales como cortafuegos y autenticación fuerte.

6.12. Seguridad de los datos

Para las copias de seguridad, adoptaremos el software de Backup Exec 22.2 (Veritas Backup Exec 16) por ser compatible con nuestro sistema operativo y para garantizarnos un proceso efectivo de recuperación en caso de pérdidas o desastres.

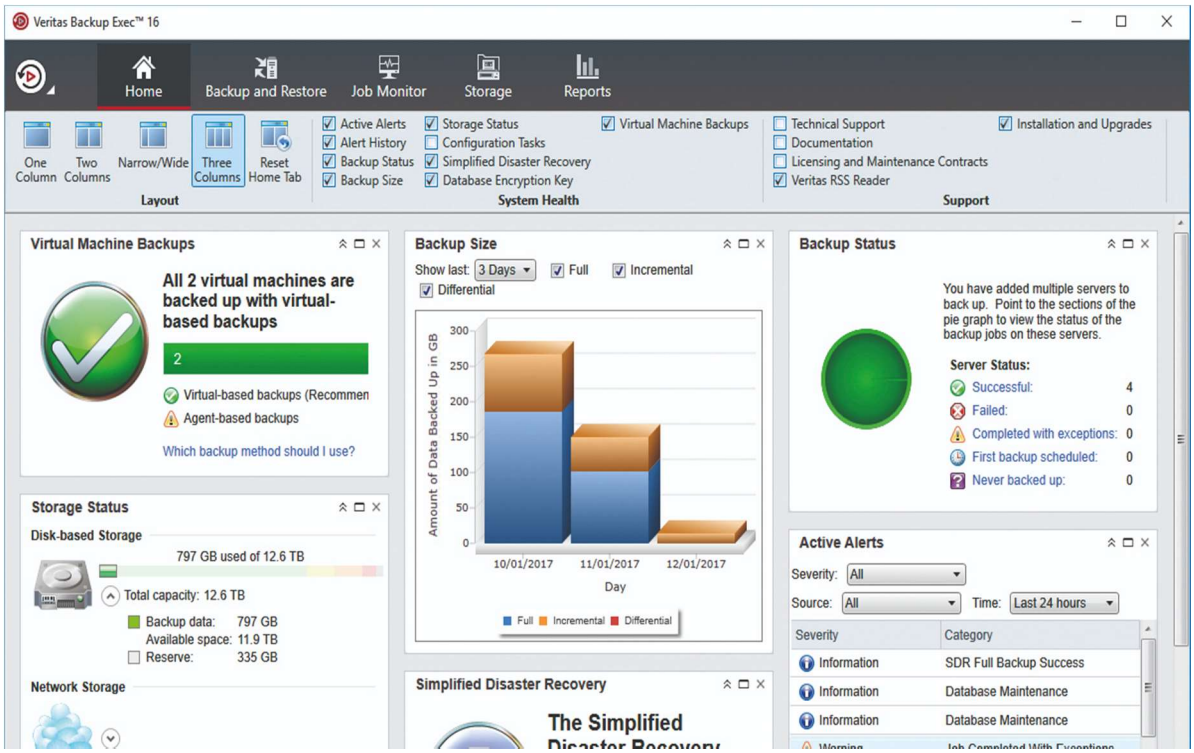

Ilustración 36. Interfaz de Veritas. Fuente: ippro.com

Configuración de copias de seguridad: Las copias de seguridad se realizaran por configuración siempre a las 23:00 horas, durante la noche, en esta empresa no hay actividades laborales o es más baja. Habrá copias de seguridad “Diarias” incrementales, “Mensuales”, “Semanales” y “Anuales” completas. Todas tendrán una infraestructura granular par recuperar los archivos perdidos o en de desastre punto a punto, sin tener que recurrir a un sistema entero o un estructura completa de archivos. Se realizaran mensualmente pruebas de recuperación para comprobar su correcto funcionamiento y las máquinas virtuales tendrán instalados agentes de Veritas para su compatibilidad c en la maquina física de copias de seguridad para salvaguardar la información que forme parte de los activos de la empresa. Asimismo, se realizaran puntos de control de las maquinas virtuales para asegurarnos en caso de desastre.

6.13. Sala de Reuniones Tecnológicamente Equipada

En la sala de reuniones se instalarán dos puertos de red dentro de la VLAN 50, uno para la tecnología VoIP y otro para la pantalla. Para la tecnología VoIP utilizaremos un Cisco IP Conference Phone 7832 porque cuenta con un servicio de conferencia, siendo adecuado para una sala de reuniones de tamaño medio, como la nuestra. Además, ofrece una interfaz fácil de usar y una óptima calidad de audio avanzada. En cuanto a la pantalla SMART Board 7075 series por su rendimiento y características avanzadas, y también, es adecuada para nuestra sala.

Ilustración 37. Modelo de Sala y dispositivo VoIP (debajo). Fuente: galiabc.es

6.14. BYOP y Flexibilidad

La adopción de política pro-BYOD (Bring Your Own Device) y la promoción de flexibilidad y modernidad en la infraestructura de red y seguridad es una estrategia importante, especialmente cuando estamos siguiendo los principios de la norma ISO 27001. Tendremos en cuanto las consideraciones siguientes:

1. **Políticas de Seguridad:** estableceremos políticas claras y detalladas relacionadas con el uso de dispositivos personales. Esto incluirá requisitos de seguridad, como tener software antivirus actualizado, configuraciones seguras, y la obligación de informar la pérdida o robo del dispositivo.

2. **Segmentación de Red:** daremos continuidad a la segmentación de red para separar el tráfico de dispositivos BYOD del tráfico de la red corporativa. Esto nos ayudará a prevenir posibles amenazas y limitará el acceso no autorizado.

3. **Autenticación Multifactor (MFA):** exigimos la autenticación multifactor para acceder a recursos críticos o sensibles, agregando una capa adicional de seguridad para proteger la información de la empresa.

4. **Gestión de Dispositivos Móviles (MDM):** implementaremos una solución de MDM para gestionar y controlar dispositivos BYOD, incluyendo la capacidad de borrar remotamente datos en caso de pérdida o robo del dispositivo y garantizar que estén configurados según las políticas de seguridad establecidas.

5. **Educación y Concienciación:** proporcionaremos capacitación y concienciación continua a los empleados sobre las mejores prácticas de seguridad para dispositivos personales, incluyendo pautas sobre el uso de contraseñas seguras, la actualización regular de software y la identificación de posibles amenazas.

6. **Control de Acceso Basado en Roles (RBAC):** implementaremos un modelo de RBAC para garantizar que los usuarios, independientemente de si utilizan dispositivos corporativos o personales, tengan acceso solo a los recursos necesarios para llevar a cabo sus funciones laborales.

7. **Auditorías y Monitorización Continua:** realizaremos auditorías regulares y monitorizamos de forma continua el tráfico y el acceso a recursos críticos. Esto nos ayudará a identificar posibles brechas de seguridad y asegurar el cumplimiento de las políticas establecidas.

8. **Cumplimiento Normativo:** nos aseguraremos que todas las políticas y prácticas adoptadas cumplen los estándares de la ISO 27001.

9. **Actualizaciones y Parches:** esto ayudará a mitigar posibles vulnerabilidades.

10. **Gestión de Incidentes:** estableceremos un plan de respuesta a incidentes que incluya procedimientos específicos para incidentes relacionados con dispositivos BYOD con la garantía de una respuesta rápida y efectiva en caso de un evento de seguridad.

6.15. Medidas contra DDoS y Acceso Biométrico

Nuestra infraestructura de red y seguridad está bien equipada y sigue las mejores prácticas de seguridad. Por tanto, las medidas que adoptaremos contra DDoS serán configurar nuestro firewall y filtros de tráfico para identificar y bloquear tráfico malicioso antes de que alcance nuestros servidores, además, utilizaremos un servicio anti-DDoS por un proveedor especializado.

En cuanto al acceso Biométrico, implementaremos la autenticación Multifactor (MFA) para agregar una capa adicional de seguridad, aunque utilicemos el acceso biométrico. Nos aseguraremos que los escáneres biométricos sean seguros y resistentes a manipulaciones. Los datos biométricos los almacenaremos de manera segura utilizando técnicas de cifrado robustas y asegurando la integridad y confidencialidad de estos datos. Aplicaremos las políticas de privacidad para establecer políticas claras sobre cómo se recopilan, almacenan y utilizan los datos biométricos, y nos aseguraremos de cumplir con las regulaciones de privacidad. Nuestro servicio incluirá el monitoreo continuo, por parte de nuestro personal especializado, de los registros biométricos para detectar posibles intentos de acceso no autorizado y, mantendremos actualizados los sistemas biométricos mediante la aplicación de parches de seguridad regularmente para mitigar vulnerabilidades conocidas.

7. Conclusiones y recomendaciones

La culminación exitosa de este proyecto representa un logro significativo en la evolución y fortalecimiento de la infraestructura tecnológica de nuestra empresa. La implementación de una infraestructura de red integral ha abordado con éxito los desafíos contemporáneos en términos de seguridad, colaboración y flexibilidad en el entorno empresarial. Paso a detallar las principales conclusiones derivadas en el proceso de la realización del proyecto.

Infraestructura Segura y Completa:

La meticulosa implementación de elementos clave, como un direccionamiento fijo privado, firewall Palo Alto, switches, routers, servidores y un Sistema de Información y Eventos de Seguridad (SIEM), respaldado por medidas de seguridad avanzadas, ha consolidado una infraestructura sólida y robusta. Esta arquitectura garantiza la confidencialidad, integridad y disponibilidad de la información, estableciendo un cimiento resistente ante las amenazas cibernéticas emergentes.

Conectividad Confiable y Medidas Proactivas:

La elección estratégica del cableado UTP y la implementación de VPNs no solo han asegurado una conectividad confiable en toda la red, sino que también reflejan un enfoque proactivo en la prevención de amenazas, destacando la importancia de salvaguardar la seguridad de la información contra potenciales ataques, como el ransomware.

Colaboración Mejorada:

La sala de reuniones tecnológicamente equipada ha revolucionado la dinámica de colaboración en la organización. Características avanzadas, como la tecnología VoIP y la capacidad para realizar reuniones virtuales, han optimizado la comunicación interna y remota, mejorando significativamente la eficiencia y la efectividad en la toma de decisiones.

Flexibilidad Laboral con Políticas Pro-BYOD:

La adopción de políticas pro-BYOD ha marcado un cambio hacia una cultura laboral más flexible y moderna. Permitir a empleados, clientes y accionistas acceder a recursos de manera segura desde sus propios dispositivos ha potenciado la flexibilidad laboral, promoviendo un entorno adaptativo en respuesta a las dinámicas cambiantes del mundo empresarial.

Compromiso con la Norma ISO 27001:

El compromiso proactivo con la norma ISO 27001 no solo demuestra la dedicación hacia los más altos estándares de seguridad de datos, sino que también destaca la implementación efectiva de medidas específicas. Esto no solo asegura la conformidad con estándares internacionales, sino que también consolida la postura de seguridad de la infraestructura.

Documentación y mantenimiento:

Se documentó toda la configuración del clúster, las configuraciones de red y almacenamiento para la posteridad. Asimismo, se indicó que se realizarán actualizaciones periódicas del sistema operativo, firmware y controladores, y realizar pruebas regulares de conmutación por error para garantizar la disponibilidad del clúster.

De manera imperativa, se deberán realizar actualizaciones regulares del sistema operativo, software, antivirus y, se deben mantener las configuraciones de seguridad apropiadas que serán implementadas por el equipo técnico encargado. No podemos terminar un proyecto, sin siempre recomendar a nuestro cliente la importancia de mantener la documentación de la configuración, políticas y procedimiento para facilitar la administración y resolución de problemas, que al menos deben ser revisadas anualmente para el debido cumplimiento con los estándares de seguridad de la ISO 27001:2022, además de las particulares por su actividad profesional, de las que serán responsables su departamento jurídico designado.

En resumen, la culminación de este proyecto no solo representa el éxito en la implementación de una infraestructura de red avanzada, sino que también sienta las bases para un futuro tecnológico sólido y adaptable, alineado con las mejores prácticas de seguridad y colaboración.

7.1. Líneas Futuras

A pesar de los logros sobresalientes, reconocemos la necesidad de una evolución continua para mantenernos a la vanguardia de la tecnología y la seguridad empresarial. Las líneas futuras delinean áreas específicas para un desarrollo continuo y una mejora constante:

Integración de Tecnologías Emergentes:

Explorar la integración de tecnologías emergentes, como inteligencia artificial y aprendizaje automático, para fortalecer la detección de amenazas y mejorar la adaptabilidad de la infraestructura a nuevas vulnerabilidades.

Optimización de Procesos con Automatización:

Implementar la automatización en procesos clave para aumentar la eficiencia operativa y reducir la carga manual en tareas repetitivas, permitiendo al equipo centrarse en actividades estratégicas.

Expansión de Capacidades Biométricas y Seguridad Física:

Considerar la expansión de las capacidades biométricas no solo en la entrada de la empresa, sino también en áreas críticas y sistemas sensibles, fortaleciendo así las medidas de seguridad física.

Evaluación Continua de Amenazas:

Establecer un programa continuo de evaluación de amenazas para mantenerse al tanto de las tácticas de ataque en constante evolución y garantizar la preparación frente a nuevas formas de riesgos cibernéticos.

Desarrollo de Capacidades de Recuperación ante Desastres:

Fortalecer las capacidades de recuperación ante desastres, incluyendo simulacros regulares y la implementación de tecnologías que minimicen el tiempo de inactividad en caso de incidentes graves.

En resumen, este proyecto no solo representa un hito en la mejora de la infraestructura tecnológica, sino que también establece una sólida base para el crecimiento futuro. La adaptación constante, la innovación tecnológica y el compromiso con la excelencia son imperativos para garantizar que la infraestructura siga siendo una columna vertebral segura y eficiente para el éxito continuo de la organización.

8. Referencias

[1] "Aplicar la norma ISO270001 y los controles ISO270002". Disponible en ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online (normaiso27001.es) Fecha del último acceso 07/12/2023

[2] "Ciclo PDCA". Disponible en ISO 27001 Paso a paso - 9 Revisión por la Dirección (normaiso27001.es). Fecha del último acceso 07/12/2023

[3] "Mejorar el grado de ciberseguridad". Disponible en CCN-CERT - Inicio (cni.es). Fecha del último acceso 07/12/2023

[4] "Cuestiones que afectan a la seguridad de la empresa". Disponible en TemáTICas | Empresas | INCIBE. Fecha del último acceso 07/12/2023

[5] "Procedimientos Recomendado VLANs". Disponible en Procedimientos recomendados de VLAN y consejos de seguridad para routers empresariales de Cisco - Cisco. Fecha del último acceso 07/12/2023

[6] "Modelo OSI". Disponible en PRORED - El modelo OSI · Origen · Capas · Ejemplos. Fecha del último acceso 07/12/2023

[7] "Switch Cisco Catalyst 2960-Plus 48PST-S". Disponible en Switch Cisco Catalyst 2960-Plus 48PST-S - Ciscos. Fecha del último acceso 07/12/2023

[8] "Routers Cisco ISR 4000". Disponible en Cisco 4000 Series Integrated Services Routers - Cisco. Fecha del último acceso 07/12/2023

[9] "Firewall Palo Alto Networks PA-820 ". Disponible en Ficha técnica de la serie PA-800 Series - Palo Alto Networks. Fecha del último acceso 07/12/2023

[10] "HPE ProLiant DL380 Gen10 ". Disponible enServidor HPE ProLiant DL380 Gen10 | HPE Store Spain. Fecha del último acceso 07/12/2023

[11] "Synology RackStation RS3618xs ". Disponible en Synology Inc.. Fecha del último acceso 07/12/2023

[13] "APC Smart-UPS. ". Disponible en Smart-UPS de APC 3000 VA LCD RM 2U 230 V - SMT3000RMI2U | APC España). Fecha del último acceso 07/12/2023

[14] "Armario El Tripp Lite SR42UBCL ". Disponible en Co-Location Standard-Depth Server Rack Cabinet 42U | Eaton. Fecha del último acceso 07/12/2023

[15] "UTP y sus códigos de colores ". Disponible enT568A y T568B: dos estándares de cable de red RJ45 | Comunidad FS . Fecha del último acceso 07/12/2023

[16] "Configuraciones ". Disponible en Routing entre VLAN con routers - CCNA desde Cero. Fecha del último acceso 07/12/2023

[18] "CCNA 1 y 2 (wordpress.com) ". Disponible en CCNA 1 y 2 (wordpress.com). Fecha del último acceso 07/12/2023

[19] "Acceso Biométrico ". Disponible en guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf (incibe.es). Fecha del último acceso 07/12/2023

[20] "BYOD ". Disponible en TemáTICas BYOD | Empresas | INCIBE. Fecha del último acceso 07/12/2023

[21] "Medidas porteccion DDoS ". Disponible en Medidas de protección frente ataques de denegación de servicio (DoS) | INCIBE-CERT | INCIBE. Fecha del último acceso 09/12/2023

[23] "AWS Site-to-Site VPN ". Disponible en ¿Qué es AWS Site-to-Site VPN? - VPN de sitio a sitio de AWS (amazon.com). Fecha del último acceso 07/12/2023

[24] "Veritas Backup ". Disponible en Backup Exec | Veritas. Fecha del último acceso 01/12/2023

[25] " Cómo configurar un clúster". Disponible en Implementación de un servidor de archivos en clúster de dos nodos | Microsoft Learn. Fecha del último acceso 07/12/2023

[26] "VoIP ". Disponible en Guía para la seguridad y el cifrado de VoIP | Ciberseguridad. Fecha del último acceso 07/12/2023

[27] "VMware Vsphere ". Disponible en Message from VMware vSphere Bot. Fecha del último acceso 07/12/2023

9. Bibliografía y webgrafía

(s.f.). Obtenido de elautonomodigital.es

(s.f.). Obtenido de https://www.paloaltonetworks.es/company

(s.f.). Obtenido de https://www.ibm.com/es-es/topics/ransomware

(s.f.). Obtenido de wikipedia.es

Aplicar la norma ISO270001 y los controles ISO270002. (05 de 12 de 2023). Obtenido de https://normaiso27001.es/

wikipedia. (2023). Obtenido de https://es.wikipedia.org/wiki/Par_trenzado_no_blindado

34, Grupo Atico. (s.f.). *protecciondatos-lopd*. Obtenido de protecciondatos-lopd.com

akami. (s.f.). Obtenido de akamai.com

aws.amazon. (s.f.). Obtenido de aws.amazon.com

Burdova, C. (2022). Obtenido de avg.com

capterra. (s.f.). Obtenido de https://www.capterra.es/glossary/118/wan-wide-area-network

colaboradores, 7. (2023). Obtenido de learn.microsoft.com

Costas Santos, J., & Raya Cabrera, J. L. (2011). *Seguridad y alta disponibilidad. Grado Superior.* Ra-ma.

Editorial, E. (2023). Obtenido de https://www.significados.com/iso/

Empey, C., & Latto, N. (2023). *avast*. Obtenido de https://www.avast.com/es-es/c-what-is-a-vpn

Fernández, Y. (2019). Obtenido de xataka.com

gesditel. (s.f.). Obtenido de https://gesditel.es/telefono-voip/

guiaspracticas. (s.f.). Obtenido de https://www.guiaspracticas.com/internet-y-redes/red-de-area-local-virtual-vlan#:~:text=Una%20red%20de%20%C3%A1rea%20local%20o%20VLAN%20%28Virtual,varias%20VLAN%20funcionando%20con%20un%20%C3%BAnico%20conmutador%20f%C3%ADsico.

Herrera, J. (2022). Obtenido de guiahardware.es

ibm. (s.f.). Obtenido de https://www.ibm.com/mx-es/topics/siem

ibm. (s.f.). Obtenido de https://www.ibm.com/es-es/topics/network-attached-storage

ionos. (s.f.). Obtenido de ionos.es

ionos. (s.f.). *ionos*. Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/direccion-ip/

Marujita. (2023). Obtenido de muytecnologicos.com/diccionario-tecnologico/servidor-de-archivos

Molina Robles, F. J., & Raya Cabrera, J. L. (2010). *Planificacióny administración de redes. Grado Superior.* Ra-ma.

Nirian, P. O. (2020). *Economipedia*. Obtenido de https://economipedia.com/definiciones/empresas/kpi-key-performance-indicator.html

Peñafiel, C. P. (2022). *Guía práctica de implementación.* Viteri C.

Techtarget, C. (2021). *computerweekly*. Obtenido de https://www.computerweekly.com/es/definicion/Calidad-de-servicio-o-QoS

vasexperts. (s.f.). Obtenido de vasexperts.com/es/resources/glossary/access-control-list/

wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host