Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Estructura Lógica



**ÍNDICE DE CONTENIDOS**

1. INTRODUCCIÓN 7

2. Estructura física y cableado estructurado 8

2.1 Tipos de medios de transmisión 8

2.2 Armarios de distribución o racks y pasacables 8

2.3 Pach-panels 8

2.4 Cableado horizontal 8

2.5 Cableado vertical 8

3. Estructura lógica 9

3.1 Topología de red 9

3.2 Direccionamiento IP y segmentación 11

4. Administración de servidores y servicios 12

4.1 Sistemas operativos y software 12

4.1.1 Servidores 12

4.1.1 Estaciones de trabajo 12

4.2 Servicios 12

4.2.1 DNS 12

4.2.2 DHCP 13

4.2.3 VPN 13

4.2.4 RADIUS 13

4.2.5 PROXY 14

5. Ciberseguridad 15

5.1 Inventario de Activos 15

5.2 Segmentación 16

5.3 ACLs trafico de red 16

5.4 Network 17

5.4.1 Firewall 17

5.4.2 Switches 17

5.4.3 DNS 18

5.4.4 VPN 19

5.4.5 IPS 19

5.4.6 RADIUS 19

5.4.7 PROXY 20

5.5 Endpoint 21

5.5.1 XDR 21

5.6 Normativa Puestos de trabajo 22

ANEXO 1. Diagrama Packet tracer 23

ANEXO 2. Conexionado Físico 24

ANEXO 3. Políticas de ciberseguridad Puestos de trabajo 29

A1.1 Contraseñas 29

A1.1.1 Resumen 29

A1.1.1 Proposito 29

A1.1.1 Audiencia 29

A1.1.2 Política 29

A1.2 Escritorio Limpio 31

A1.2.1 Resumen 31

A1.2.2 Propósito 31

A1.2.3 Política 31

A1.3 Uso del correo electrónico 32

A1.3.1 Resumen 32

A1.3.2 Propósito 32

A1.3.3 Audiencia 32

A1.3.4 Legal 32

A1.3.5 Política 32

A1.3.6 Uso incidental 34

A1.3.7 Retención de correos 34

A1.3.8 Archivado de correos 34

A1.4 Actualizaciones 35

A1.4.1 Resumen 35

A1.4.2 Propósito 35

A1.4.3 Audiencia 35

A1.4.4 Detalles de la política 35

A1.5 Redes sociales 36

A1.5.1 Descripción 36

A1.5.2 Propósito de las redes sociales 36

A1.5.3 política 37

ANEXO 4. Pulseway 41

A1.6 Administración de dispositivos 41

A1.6.1 Descubrimiento y despliegue 41

A1.6.2 Monitorización y administración 42

A1.6.3 Automatización y auto remediación 43

A1.6.4 Administración de parches de seguridad 44

A1.6.5 Detección de Ransomware y AV integrado 45

A1.7 Backup & Disaster Recovery 46

A1.8 Protección contra Ransomware 47

A1.8.1 Protección contra Phishing 47

A1.8.2 Planes de concienciación 48

A1.8.3 Escáner de vulnerabilidades 49

A1.8.4 Backup and Disaster Recovery 50

GLOSARIO 51

 ABREVIATURAS Y ACRÓNIMOS 51

 DEFINICIONES 51

CONTROL DE CAMBIOS 52

**ÍNDICE DE TABLAS:**

Tabla 1‑1 Departamentos 7

Tabla 3‑1 Direccionamiento y segmentación 11

Tabla 5‑1 Conexionado Físico 28

**ÍNDICE DE FIGURAS:**

Figura 3‑1 Topología de núcleo colapsado 9

Figura 3‑1 Diagrama conceptual 10

Figura 5‑1 Diagrama Físico planta superior 23

Figura 5‑2 Diagrama Físico planta inferior 23

Figura 5‑3 Pulseway endpoint discovery 41

Figura 5‑4 Monitorización y Administración 42

Figura 5‑5 Automatizaciones 43

Figura 5‑6 Parches de Seguridad 44

Figura 5‑7 Detección de Ransomware 45

Figura 5‑8 Backup & Disaster Recovery 46

Figura 5‑9 Phishing 47

Figura 5‑10 Planes de concienciación 48

Figura 5‑11 Escáner de vulnerabilidades 49

Figura 5‑12 Backup & Disaster Recovery 50

# INTRODUCCIÓN

En este documento se va a detallar la estructura lógica de la empresa Bionica Automations.

La empresa estará ubicada en el polígono de Plaza Zaragoza, sitio elegido por ser un enclave logístico sin igual.

A continuación, vamos a realizar el diseño de una red informática de la empresa.

La empresa tiene un edificio de 2 plantas donde hay que realizar el diseño de la red para los departamentos que confirman la empresa y dimensionar las redes acordes a las necesidades requeridas:

|  |  |
| --- | --- |
| Departamento | Personal |
| Sistemas | 5 |
| Comercial | 6 |
| Soporte | 8 |
| Contabilidad | 6 |
| Dirección | 4 |
| Recursos Humanos | 4 |
| I+D | 36 |

Tabla ‑ Departamentos

# Estructura física y cableado estructurado

## Tipos de medios de transmisión

Los medios de transmisión escogidos para el proyecto han sido: fibra óptica de 10 Gb para las comunicaciones entre los dispositivos del CPD y el cableado vertical, cable de par trenzado CAT-7 para el cableado horizontal y el aire (WiFi): bandas de 2.4 estándar IEEE 802.11n y 5 GHz IEEE 802.11ac.

## Armarios de distribución o racks y pasacables

Para el CPD hay un rack donde están todos los equipos junto con 2 pasacables laterales que recorren el rack de arriba abajo con 3 paneles de parcheo.

Para la planta baja hay un armario de distribución que contiene un panel de parcheo y un switch para abastecer a la planta.

## Pach-panels

En el siguiente documento está el mapeado de las bocas del panel de parcheo a las respectivas bocas de las rosetas identificadas por “S1, S2, S3” en caso de que pertenezcan a la planta superior o “B1, B2, B3” si son de la planta baja.

## Cableado horizontal

Para el cableado horizontal vamos a utilizar cable de par trenzado CAT-6 con rosetas en cada zona de trabajo numeradas con la nomenclatura.

Todos los cables se pasarán por el suelo o techo técnicos, dependiendo de lo que haya disponible con sus respectivos aislantes para evitar las interferencias, eso supone canaletas especiales dependiendo si los cables pasan al lado de los cables eléctricos.

## Cableado vertical

Para el cableado vertical hemos optado por cables de fibra plástica de 10 Gb de ancho de banda para evitar cuellos de botella en la red y porque es fácil de manejar debido a que no necesitan de canalizaciones especiales como el cable de par trenzado, al no ser impulsos eléctricos le que va a viajar por esos cables, se pueden ubicar justo al lado de los cables eléctricos sin que haya ninguna interferencia, por lo que se pueden aprovechar las canalizaciones ya existentes.

# Estructura lógica

## Topología de red

La topología de la red se compone de un núcleo/distribución colapsado, es decir, la capa del núcleo y distribución se unen para formar una, de esta manera se simplifica la red, se reducen costes y se aumenta la eficiencia.

La red se segmenta por VLANs que van en función de los departamentos existentes.

Diagrama

Descripción generada automáticamente

Figura ‑ Topología de núcleo colapsado

A continuación, se muestra un esquema de la red de la empresa:

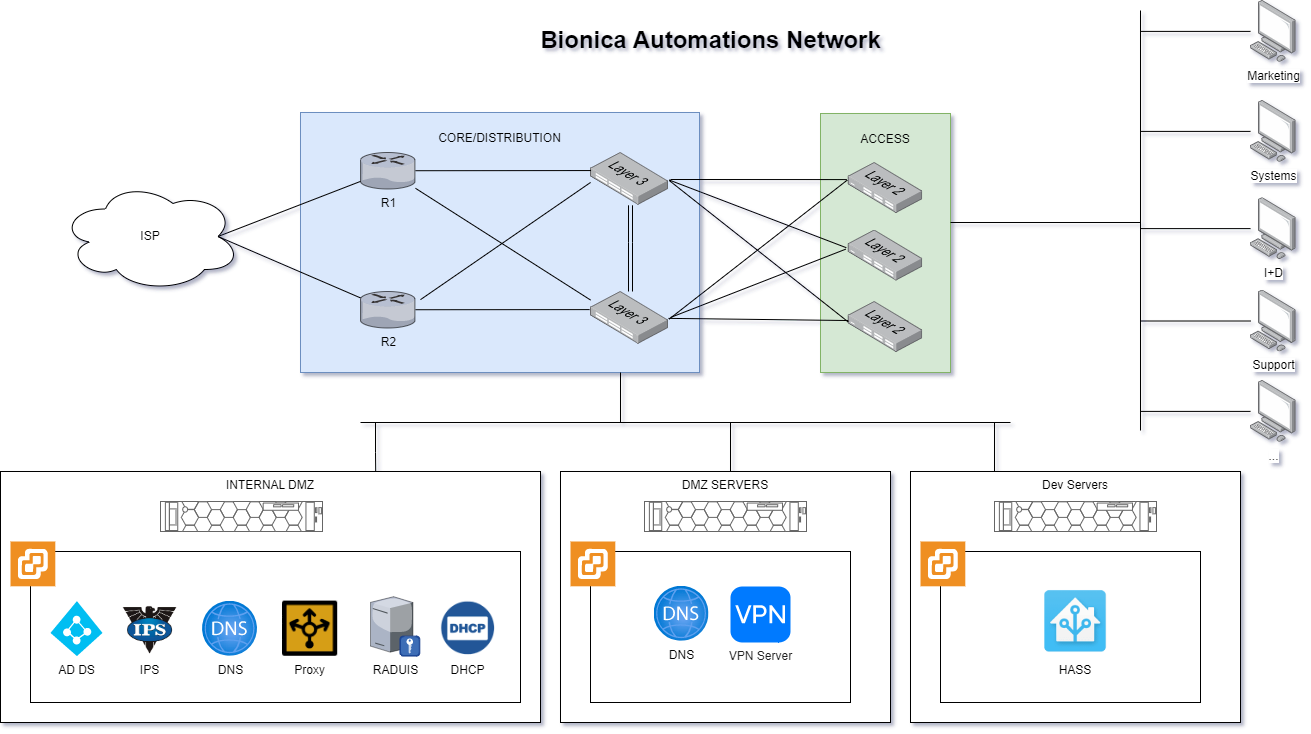


Figura ‑ Diagrama conceptual

## Direccionamiento IP y segmentación

Se ha optado por segmentar la red por departamentos para a sí minimizar el impacto que pueda tener un futuro ataque con malware u otro tipo a la red corporativa.

En la siguiente tabla se lleva a cabo el direccionamiento de las redes de la empresa:

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Name | Network IP | DHCP |
| 10 | WiFi Empleados | N/A | N/A |
| 15 | WiFi Guest | 192.168.15.0/24 | 192.168.15.11-230  240 IPs |
| 20 | Demo\_Area | 192.168.20.0/24 | 192.168.20. 11 - 50  40 IPs |
| 30 | I+D | 192.168.30.0/24 | 192.168.30. 11 - 70  60 IPs |
| 49 | Native-Trunk | N/A | N/A |
| 50 | Systems | 192.168.50.0/24 | 192.168.50.11 - 50  40 IPs |
| 60 | Commercial | 192.168.60.0/24 | 192.168.60.11 - 50  40 IPs |
| 70 | Accounting | 192.168.70.0/24 | 192.168.60.11 - 50  40 IPs |
| 80 | Support | 192.168.80.0/24 | 192.168.70.11 - 50  40 IPs |
| 90 | R-H | 192.168.90.0/24 | 192.168.90.11 - 50  40 IPs |
| 99 | Management | 192.168.99.0/24 | N/A |
| 100 | Direction | 192.168.100.0/24 | 192.168.100.11 - 50  40 IPs |
| 110 | Testing | 192.168.110.0/24 | N/A |
| 120 | Printers | 192.168.120.0/24 | N/A |
| 150 | Internal DMZ | 192.168.150.0/24 | N/A |
| 200 | DMZ | 192.168.200.0/24 | N/A |
| 555 | Black-Hole | N/A | N/A |
| 666 | RADIUS-SWAP | N/A | N/A |

Tabla ‑ Direccionamiento y segmentación

# Administración de servidores y servicios

## Sistemas operativos y software

### Servidores

Como software de virtualización se usará VMware vSphere Hypervisor (ESXi) junto con VMware vCenter.

Se dispondrá de un Windows Server 2022 standard como controlador de dominio con redundancia en Azure.

### Estaciones de trabajo

Los ordenadores de los trabajadores llevan Windows 10 Pro y se administrarán con el controlador de dominio además de Pulseway.

## Servicios

### DNS

Un servidor DNS interno en una empresa se utiliza para proporcionar servicios de resolución de nombres de dominio a los dispositivos de la red interna de la empresa. Cuando un dispositivo dentro de la red necesita comunicarse con otro dispositivo o recurso dentro de la misma red, utiliza un nombre de dominio para referirse a ese dispositivo o recurso. El servidor DNS interno traduce ese nombre de dominio en una dirección IP numérica que se utiliza para establecer la conexión.

Un servidor DNS interno puede ser configurado para almacenar una copia local de los registros de resolución de nombres de dominio para los dominios que se utilizan con frecuencia dentro de la red de la empresa. Al almacenar estos registros de forma local, se reduce la necesidad de realizar consultas DNS a través de Internet, lo que puede mejorar la velocidad de respuesta y reducir la carga en la conexión a Internet.

Además, un servidor DNS interno también puede ser configurado para restringir el acceso a ciertos nombres de dominio o para bloquear el acceso a sitios web maliciosos o no autorizados. Esto se logra mediante la configuración de políticas de seguridad y filtrado de DNS en el servidor DNS.

En cuanto a la administración de la red, el servidor DNS interno puede ser administrado por el personal de TI de la empresa para garantizar que los registros de resolución de nombres de dominio sean precisos y estén actualizados. También puede ser utilizado para crear y administrar nombres de dominio personalizados para los servicios y recursos internos, lo que facilita el acceso a estos recursos para los usuarios de la empresa.

### DHCP

El servidor DHCP permite la asignación automática de direcciones IP a los dispositivos de red, lo que simplifica la administración y reduce la posibilidad de errores humanos.

Con un servidor DHCP, la asignación de direcciones IP a los dispositivos de red se automatiza. Esto significa que los administradores de red no tienen que preocuparse por configurar manualmente cada dispositivo individualmente, lo que puede ser especialmente útil en redes grandes con muchos dispositivos.

Cuando las direcciones IP se asignan manualmente, existe la posibilidad de cometer errores. Un servidor DHCP elimina este riesgo, ya que las direcciones IP se asignan automáticamente.

Al automatizar la asignación de direcciones IP, se ahorra tiempo que se podría usar en otras tareas de administración de red.

Con DHCP, los dispositivos de red pueden moverse de una ubicación a otra y aun así recibir una dirección IP válida. Esto es particularmente útil para dispositivos inalámbricos, como laptops y teléfonos móviles, que se mueven de una red a otra.

La configuración de DHCP se realiza en un solo lugar, el servidor DHCP. Esto hace que sea fácil configurar y cambiar las opciones de red, como la dirección del servidor DNS y la puerta de enlace predeterminada.

### VPN

Una VPN puede ser utilizada para permitir a los empleados acceder de forma segura a los recursos de la empresa desde ubicaciones remotas, como desde sus hogares o mientras están en viaje de negocios. También puede permitir que los empleados se conecten a redes privadas virtuales (VPN) de otras empresas o sucursales de la misma empresa.

### RADIUS

RADIUS es un protocolo de red utilizado para autenticar, autorizar y contabilizar el acceso de los usuarios a una red, especialmente en redes de área amplia y redes inalámbricas.

Al utilizar RADIUS, un servidor RADIUS autentica las credenciales del usuario y autoriza o deniega el acceso según la información de autorización configurada.

### PROXY

Es un tipo de servidor que actúa como intermediario entre los dispositivos de la red interna de la empresa y los servidores en Internet. Cuando un dispositivo de la red intenta acceder a una página web o un recurso en línea, en lugar de conectarse directamente a Internet, la solicitud se envía al servidor proxy, que luego se encarga de hacer la solicitud en nombre del dispositivo.

El servidor proxy se puede configurar para realizar varias funciones, como filtrar el tráfico web, acelerar la carga de páginas web y proteger la privacidad y la seguridad de los dispositivos de la red interna de la empresa.

# Ciberseguridad

## Inventario de Activos

El software que va a emplear Bionica Automations para mantener un seguimiento de los equipos informáticos de la empresa va a ser [Pulseway](https://www.pulseway.com).

Pulseway es una herramienta no solo ofrece la posibilidad de hacer un inventario de inventariado, sino que también monitoriza, automatiza, protege y gestiona los activos de la empresa.

Esta herramienta es de pago, se pueden consultar sus precios por dispositivo en su [calculadora online.](https://www.pulseway.com/pricing)

Entre las características que incluye este software están las siguientes:

* [Administración de dispositivos](https://www.pulseway.com/it-management-software)
* [Backup & Disaster Recovery](https://www.pulseway.com/backup-software)
* [Protección contra Ransomware](https://www.pulseway.com/ransomware-protection-software)

Para más información consultar el **ANEXO 4 Pulseway**

## Segmentación

La segmentación de redes es un proceso que implica dividir una red grande en redes más pequeñas, conocidas como segmentos. Cada segmento de red tiene su propia dirección IP y está diseñado para ser independiente de los otros segmentos de la red.

La segmentación de redes es esencial para mejorar la seguridad de la red. Al separar diferentes tipos de tráfico en segmentos de red separados, se puede controlar y limitar el acceso a recursos críticos de la red. En caso de un ataque en un segmento de red, la segmentación de la red ayuda a limitar el impacto a otros segmentos de la red.

Al segmentar la red, se reduce la complejidad de la administración de la red. Cada segmento de red puede ser administrado de manera independiente, lo que facilita la identificación y solución de problemas y la implementación de políticas de seguridad.

La segmentación de redes ayuda a optimizar el rendimiento de la red al reducir la congestión y mejorar la eficiencia del tráfico de red. Al separar diferentes tipos de tráfico en segmentos de red separados, se puede garantizar que el tráfico crítico tenga prioridad y que no se interrumpa por otros tipos de tráfico.

La segmentación de redes es una buena práctica de seguridad y se recomienda por muchas regulaciones y estándares de seguridad, como PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) y GDPR (General Data Protection Regulation). Cumplir con estas regulaciones y estándares es importante para proteger la información confidencial de la empresa y evitar multas y sanciones.

## ACLs trafico de red

Por defecto las VLANs de los distintos departamentos no se comunican, al único punto en común al que tiene acceso es a la red de INTERNAL-DMZ donde se hace un filtrado por departamento de los recursos que necesita acceder de esa red.

Los equipos autorizados por el servidor RAIDUS tendrán acceso a internet a través de un servidor PROXY situado en la INTERNAL-DMZ, ningún equipo de la red estará autorizado a salir a internet directamente salvo excepciones.

## Network

Para reforzar la protección de la infraestructura de red se seguirán las recomendaciones de la siguiente guía:

* [NSA\_NETWORK\_INFRASTRUCTURE\_SECURITY\_GUIDE](https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF)

### Firewall

Para fortalecer la seguridad de la infraestructura de red se ha elegido la siguiente guía

* [CSI\_CISCO\_PASSWORD\_TYPES\_BEST\_PRACTICES](https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF)

### Switches

Siguiendo el estándar 802.1X los switches de la capa de acceso estarán configurados con un filtrado MAC, además de autenticación con el servidor de RADIUS.

Los clientes que no se autentiquen contra el servidor de autenticación RADIUS caerán rechazados a la VLAN 555 Black-Hole, donde no podrán acceder a ningún recurso de la empresa.

Además, para estos dispositivos también se seguirá la guía de seguridad en infraestructuras mencionada en el apartado **5.2 Segmentación**

La segmentación de redes es un proceso que implica dividir una red grande en redes más pequeñas, conocidas como segmentos. Cada segmento de red tiene su propia dirección IP y está diseñado para ser independiente de los otros segmentos de la red.

La segmentación de redes es esencial para mejorar la seguridad de la red. Al separar diferentes tipos de tráfico en segmentos de red separados, se puede controlar y limitar el acceso a recursos críticos de la red. En caso de un ataque en un segmento de red, la segmentación de la red ayuda a limitar el impacto a otros segmentos de la red.

Al segmentar la red, se reduce la complejidad de la administración de la red. Cada segmento de red puede ser administrado de manera independiente, lo que facilita la identificación y solución de problemas y la implementación de políticas de seguridad.

La segmentación de redes ayuda a optimizar el rendimiento de la red al reducir la congestión y mejorar la eficiencia del tráfico de red. Al separar diferentes tipos de tráfico en segmentos de red separados, se puede garantizar que el tráfico crítico tenga prioridad y que no se interrumpa por otros tipos de tráfico.

La segmentación de redes es una buena práctica de seguridad y se recomienda por muchas regulaciones y estándares de seguridad, como PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) y GDPR (General Data Protection Regulation). Cumplir con estas regulaciones y estándares es importante para proteger la información confidencial de la empresa y evitar multas y sanciones.

## ACLs trafico de red

Por defecto las VLANs de los distintos departamentos no se comunican, al único punto en común al que tiene acceso es a la red de INTERNAL-DMZ donde se hace un filtrado por departamento de los recursos que necesita acceder de esa red.

Los equipos autorizados por el servidor RAIDUS tendrán acceso a internet a través de un servidor PROXY situado en la INTERNAL-DMZ, ningún equipo de la red estará autorizado a salir a internet directamente salvo excepciones.

Network.

### DNS

Para proteger nuestro servidor DNS interno se han tomado las siguientes guías de referencia:

* [CSI\_ADOPTING\_ENCRYPTED\_DNS](https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF)

En la guía se tratan los siguientes puntos para encriptar las consultas DNS:

* Implementar protocolos de DNS cifrados como DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT) para cifrar consultas y respuestas DNS.
* Configurar el servidor DNS para que solo acepte consultas cifradas.
* Utilizar un servidor DNS que permita la implementación de políticas de seguridad, como bloquear consultas a sitios web maliciosos.
* Implementar medidas de autenticación y autorización para evitar que usuarios no autorizados accedan al servidor DNS.
* Limitar el acceso al servidor DNS solo a usuarios autorizados y aplicaciones que necesiten acceder a él.

El objetivo de la siguiente guía es proporcionar información y recomendaciones para que las organizaciones puedan seleccionar y configurar servicios de Sistema de Nombres de Dominio (DNS) de protección para mejorar la seguridad de sus redes y protegerse contra ciberataques. El documento describe los diferentes tipos de servicios de DNS de protección disponibles, sus características y criterios para su selección y configuración. También incluye información sobre consideraciones técnicas y operativas, así como pautas para la implementación de un servicio de DNS de protección en una red.

* [CSI Selecting Protective DNS Service](https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting%20a%20Protective%20DNS%20Service_U00117652-21.PDF)

### VPN

En la empresa se dispone de un servidor VPN Ipsec para que los trabajadores puedan conectarse y usar los recursos de la empresa desde sus casas, como pueden ser acceso a infraestructura de pruebas y entornos de desarrollo.

Para la configuración de los túneles IPsec se utilizará la siguiente guía:

* [Configuring\_IPsec\_VPN](https://media.defense.gov/2020/Jul/02/2002355501/-1/-1/0/Configuring_IPsec_VPN_UOO148260_20_V1_2.PDF)

Luego para otras conexiones más comunes como el acceso al portal de gestión de tareas, u otros servicios web se utilizará una implementación de túneles con Cloud Flare que permiten el acceso a aplicaciones internas a través desde internet. Para más información consultar el siguiente enlace: <https://www.cloudflare.com/es-es/products/tunnel/>

### IPS

Un IPS trabaja en tiempo real para identificar y bloquear actividades maliciosas en una red, como intentos de hacking, malware, phishing, ataques de denegación de servicio (DDoS) y otras amenazas. Utiliza técnicas como la detección de firmas, el análisis de comportamiento y la inspección profunda de paquetes para identificar actividades sospechosas y tomar medidas para prevenir el ataque.

Además de detectar y bloquear las amenazas, un IPS también puede generar alertas y registros para informar a los administradores de la red sobre los posibles ataques y proporcionar información para la investigación y resolución de incidentes de seguridad.

### RADIUS

Cuando un usuario intenta acceder a la red a través de un puerto de switch configurado para utilizar RADIUS, el switch envía una solicitud de autenticación al servidor RADIUS. Si la autenticación es exitosa, el servidor RADIUS envía una respuesta al switch con la información de autorización, incluyendo la VLAN a la que se debe asignar el usuario.

Si el servidor RADIUS deniega el acceso del usuario, el switch asignará al usuario a la VLAN 555 Black-Hole, que es una VLAN de rechazo que puede estar configurada para limitar el acceso del usuario a la red o impedir completamente el acceso.

Durante este proceso, el switch utilizar una VLAN de intercambio, 666 RADIUS-SWAP, para mover temporalmente el tráfico del usuario a esa VLAN mientras se realiza el cambio a la VLAN de destino. Una vez que se ha completado la autenticación y la autorización del usuario, el switch moverá el tráfico del usuario a la VLAN correspondiente.

### PROXY

Un servidor proxy es un servidor que actúa como intermediario entre los clientes de la red y los servidores externos. Al enrutar las solicitudes de los clientes a través del servidor proxy, se pueden proporcionar ciertos beneficios de seguridad para una red empresarial, tales como:

Control de acceso a Internet: Un servidor proxy puede ser utilizado para controlar el acceso a Internet de los empleados y limitar el acceso a sitios web no autorizados o inapropiados. El servidor proxy puede implementar políticas de seguridad que restringen el acceso a ciertos sitios web o tipos de contenido, lo que puede ayudar a prevenir amenazas cibernéticas, como el malware o el phishing.

Mejora de la privacidad y seguridad: Al enrutar todas las solicitudes de los clientes a través del servidor proxy, se puede mejorar la privacidad y seguridad de la red empresarial. El servidor proxy puede filtrar y bloquear el tráfico malicioso antes de que llegue a la red empresarial, lo que ayuda a proteger contra ataques y amenazas cibernéticas.

Aceleración del rendimiento: Un servidor proxy también puede mejorar el rendimiento de la red empresarial al almacenar en caché el contenido web más utilizado. Esto significa que cuando un usuario solicita una página web, el servidor proxy puede devolver la página almacenada en caché en lugar de volver a descargarla desde Internet, lo que puede acelerar el tiempo de carga y reducir el ancho de banda necesario.

Registro y análisis de tráfico: Un servidor proxy puede ser utilizado para registrar y analizar todo el tráfico web en la red empresarial. Esto puede ser útil para los administradores de la red para identificar y solucionar problemas de red, para hacer cumplir las políticas de seguridad y para detectar posibles amenazas.

## Endpoint

### XDR

Se piensa instalar un software XDR para proteger los equipos de los trabajadores.

Un XDR es una solución de seguridad de próxima generación que combina datos de múltiples fuentes para proporcionar una visibilidad completa de la infraestructura de una organización y detectar y responder a las amenazas cibernéticas de manera más efectiva. Esto permite a los equipos de seguridad tomar decisiones más rápidas y reducir el tiempo de respuesta a las amenazas cibernéticas.

La principal característica de un XDR es que combina datos de múltiples fuentes, incluyendo el endpoint, la red y la nube, para proporcionar una visibilidad completa de la infraestructura de una organización. Utiliza inteligencia artificial y aprendizaje automático para analizar estos datos y detectar patrones y comportamientos anormales que pueden ser indicativos de una amenaza cibernética.

Algunas de las principales ventajas de un XDR desde un punto de vista de ciberseguridad son las siguientes:

Mayor visibilidad: al integrar datos de múltiples fuentes, un XDR proporciona una visibilidad completa de la infraestructura de una organización, lo que permite una detección y respuesta más rápida y efectiva a las amenazas cibernéticas.

Detección y respuesta más rápidas: con la capacidad de analizar grandes cantidades de datos en tiempo real, un XDR puede detectar y responder a las amenazas cibernéticas más rápidamente que las soluciones de seguridad tradicionales.

Reducción de falsos positivos: al utilizar inteligencia artificial y aprendizaje automático, un XDR puede reducir la cantidad de falsos positivos generados por las soluciones de seguridad tradicionales, lo que permite a los equipos de seguridad centrarse en las amenazas reales.

Automatización de la respuesta: un XDR puede automatizar la respuesta a las amenazas cibernéticas, permitiendo que los equipos de seguridad respondan a las amenazas de manera más rápida y efectiva.

## Normativa Puestos de trabajo

Las políticas aplicables al puesto de trabajo están descritas en el siguiente anexo:

**ANEXO 3 Políticas de ciberseguridad Puestos de trabajo**

1. Diagrama Packet tracer

El esquema está en formato Packet Tracert [Diagrama Packet Tracer](Anexos/Anexo%201%20-%20Diagrama%20Packet%20Tracer)

Imagen que contiene interior, edificio, computadora, montón

Descripción generada automáticamente

Figura ‑ Diagrama Físico planta superior

Diagrama, Dibujo de ingeniería

Descripción generada automáticamente

Figura ‑ Diagrama Físico planta inferior

1. Conexionado Físico

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Device | Port | VLAN | Use | Conected Device | Target Port | Patch Panel | Patch Panel Port |
| R\_Movistar | g0/0/0 | N/A | WAN 1 | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/0/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/0/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/0 | Trunk 49 | Internet | SW\_C1 | g1/1/4 | N/A | N/A |
| R\_Movistar | g0/1/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/3 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/0 | N/A | WAN 2 | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/0 | Trunk 49 | Internet | SW\_C2 | g1/1/4 | N/A | N/A |
| R\_Vodafone | g0/1/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/3 | N/A | N/A | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/1 | Trunk | Connunication | SW\_P1-1 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/2 | Trunk | Connunication | SW\_P1-2 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/3 | Trunk | Connunication | SW\_P1-3 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/4 | Trunk | Connunication | SW\_P0-1 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/12 | 99 | MGM ESXi | ESXi\_1 | g0 | N/A | N/A |
| SW\_C1 | g1/0/13 | 150 | Internal Services | ESXi\_1 | g1 | N/A | N/A |
| SW\_C1 | g1/0/14 | 150 | Servers | NAS | g0 | N/A | N/A |
| SW\_C1 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/21 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/22 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/23 | Trunk | Communication | SW\_C2 | g1/0/23 | N/A | N/A |
| SW\_C1 | g1/0/24 | Trunk | Communication | SW\_C2 | g1/0/24 | N/A | N/A |
| SW\_C1 | g1/1/1 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/4 | Trunk | Connunication | Router\_Movistar | g0/0/1 | N/A | N/A |
| SW\_C2 | g1/0/1 | Trunk | Connunication | SW\_P1-1 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/2 | Trunk | Connunication | SW\_P1-2 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/3 | Trunk | Connunication | SW\_P1-3 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/4 | Trunk | Connunication | SW\_P0-1 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/12 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/13 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/14 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/21 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/22 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/23 | Trunk | Communication | SW\_C1 | g1/0/23 | N/A | N/A |
| SW\_C2 | g1/0/24 | Trunk | Communication | SW\_C1 | g1/0/24 | N/A | N/A |
| SW\_C2 | g1/1/1 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/4 | Trunk | Communication | Router\_Vodafone | g0/0/1 | N/A | N/A |
| SW\_P1-1 | g1/0/1 | 30 | Developers | Roseta\_S9 | 0 | Patch\_Panel\_S1 | 1 |
| SW\_P1-1 | g1/0/2 | 30 | Developers | Roseta\_S9 | 1 | Patch\_Panel\_S1 | 2 |
| SW\_P1-1 | g1/0/3 | 30 | Developers | Roseta\_S9 | 2 | Patch\_Panel\_S1 | 3 |
| SW\_P1-1 | g1/0/4 | 30 | Developers | Roseta\_S9 | 3 | Patch\_Panel\_S1 | 4 |
| SW\_P1-1 | g1/0/5 | 30 | Developers | Roseta\_S10 | 0 | Patch\_Panel\_S1 | 5 |
| SW\_P1-1 | g1/0/6 | 30 | Developers | Roseta\_S10 | 1 | Patch\_Panel\_S1 | 6 |
| SW\_P1-1 | g1/0/7 | 30 | Developers | Roseta\_S10 | 0 | Patch\_Panel\_S1 | 7 |
| SW\_P1-1 | g1/0/8 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 8 |
| SW\_P1-1 | g1/0/9 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 9 |
| SW\_P1-1 | g1/0/10 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 10 |
| SW\_P1-1 | g1/0/11 | 30 | Developers | Roseta\_S12 | 0 | Patch\_Panel\_S1 | 11 |
| SW\_P1-1 | g1/0/12 | 30 | Developers | Roseta\_S12 | 1 | Patch\_Panel\_S1 | 12 |
| SW\_P1-1 | g1/0/13 | 30 | Developers | Roseta\_S12 | 2 | Patch\_Panel\_S1 | 13 |
| SW\_P1-1 | g1/0/14 | 30 | Developers | Roseta\_S12 | 3 | Patch\_Panel\_S1 | 14 |
| SW\_P1-1 | g1/0/15 | 30 | Developers | Roseta\_S13 | 0 | Patch\_Panel\_S1 | 15 |
| SW\_P1-1 | g1/0/16 | 30 | Developers | Roseta\_S13 | 1 | Patch\_Panel\_S1 | 16 |
| SW\_P1-1 | g1/0/17 | 30 | Developers | Roseta\_S13 | 2 | Patch\_Panel\_S1 | 17 |
| SW\_P1-1 | g1/0/18 | 30 | Developers | Roseta\_S13 | 3 | Patch\_Panel\_S1 | 18 |
| SW\_P1-1 | g1/0/19 |  | Phones | Roseta\_S14 | 0 | Patch\_Panel\_S1 | 19 |
| SW\_P1-1 | g1/0/20 |  | Phones | Roseta\_S14 | 1 | Patch\_Panel\_S1 | 20 |
| SW\_P1-1 | g1/0/21 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/22 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/23 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/24 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/1 | N/A | N/A |
| SW\_P1-1 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/1 | N/A | N/A |
| SW\_P1-1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-2 | g1/0/1 | 50 | Systems-Admin | Roseta\_S0 | 0 | Patch\_Panel\_S2 | 1 |
| SW\_P1-2 | g1/0/2 | 50 | Systems-Admin | Roseta\_S0 | 1 | Patch\_Panel\_S2 | 2 |
| SW\_P1-2 | g1/0/3 | 50 | Systems-Admin | Roseta\_S0 | 2 | Patch\_Panel\_S2 | 3 |
| SW\_P1-2 | g1/0/4 | 50 | Systems-Admin | Roseta\_S0 | 3 | Patch\_Panel\_S2 | 4 |
| SW\_P1-2 | g1/0/5 | 50 | Systems-Admin | Roseta\_S1 | 0 | Patch\_Panel\_S2 | 5 |
| SW\_P1-2 | g1/0/6 | 555 | Not Used | Roseta\_S1 | 1 | Patch\_Panel\_S2 | 6 |
| SW\_P1-2 | g1/0/7 | 110 | Testing | Roseta\_S2 | 0 | Patch\_Panel\_S2 | 7 |
| SW\_P1-2 | g1/0/8 | 110 | Testing | Roseta\_S3 | 0 | Patch\_Panel\_S2 | 8 |
| SW\_P1-2 | g1/0/9 | 110 | Testing | Roseta\_S4 | 0 | Patch\_Panel\_S2 | 9 |
| SW\_P1-2 | g1/0/10 | 90 | R-H | Roseta\_S5 | 0 | Patch\_Panel\_S2 | 10 |
| SW\_P1-2 | g1/0/11 | 80 | Call-Center | Roseta\_S6 | 0 | Patch\_Panel\_S2 | 11 |
| SW\_P1-2 | g1/0/12 | 80 | Call-Center | Roseta\_S6 | 1 | Patch\_Panel\_S2 | 12 |
| SW\_P1-2 | g1/0/13 | 80 | Call-Center | Roseta\_S6 | 2 | Patch\_Panel\_S2 | 13 |
| SW\_P1-2 | g1/0/14 | 80 | Call-Center | Roseta\_S6 | 3 | Patch\_Panel\_S2 | 14 |
| SW\_P1-2 | g1/0/15 | 80 | Call-Center | Roseta\_S7 | 0 | Patch\_Panel\_S2 | 15 |
| SW\_P1-2 | g1/0/16 | 80 | Call-Center | Roseta\_S7 | 1 | Patch\_Panel\_S2 | 16 |
| SW\_P1-2 | g1/0/17 | 80 | Call-Center | Roseta\_S7 | 2 | Patch\_Panel\_S2 | 17 |
| SW\_P1-2 | g1/0/18 | 80 | Call-Center | Roseta\_S7 | 3 | Patch\_Panel\_S2 | 18 |
| SW\_P1-2 | g1/0/19 | 70 | Accounting | Roseta\_S8 | 0 | Patch\_Panel\_S2 | 19 |
| SW\_P1-2 | g1/0/20 | 70 | Accounting | Roseta\_S8 | 1 | Patch\_Panel\_S2 | 20 |
| SW\_P1-2 | g1/0/21 | 70 | Accounting | Roseta\_S8 | 2 | Patch\_Panel\_S2 | 21 |
| SW\_P1-2 | g1/0/22 | 70 | Accounting | Roseta\_S8 | 3 | Patch\_Panel\_S2 | 22 |
| SW\_P1-2 | g1/0/23 | 70 | Accounting | Roseta\_S20 | 0 | Patch\_Panel\_S2 | 23 |
| SW\_P1-2 | g1/0/24 | 70 | Accounting | Roseta\_S20 | 1 | Patch\_Panel\_S2 | 24 |
| SW\_P1-2 | g1/1/1 | Trunk | Connunication | SW\_C1 | g1/0/2 | N/A | N/A |
| SW\_P1-2 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/2 | N/A | N/A |
| SW\_P1-2 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-2 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/1 | 40 | Programers | Roseta\_S15 | 0 | Patch\_Panel\_S3 | 1 |
| SW\_P1-3 | g1/0/2 | 40 | Programers | Roseta\_S15 | 1 | Patch\_Panel\_S3 | 2 |
| SW\_P1-3 | g1/0/3 | 40 | Programers | Roseta\_S15 | 2 | Patch\_Panel\_S3 | 3 |
| SW\_P1-3 | g1/0/4 | 40 | Programers | Roseta\_S15 | 3 | Patch\_Panel\_S3 | 4 |
| SW\_P1-3 | g1/0/5 | 40 | Programers | Roseta\_S16 | 0 | Patch\_Panel\_S3 | 5 |
| SW\_P1-3 | g1/0/6 | 40 | Programers | Roseta\_S16 | 1 | Patch\_Panel\_S3 | 6 |
| SW\_P1-3 | g1/0/7 | 40 | Programers | Roseta\_S16 | 2 | Patch\_Panel\_S3 | 7 |
| SW\_P1-3 | g1/0/8 | 40 | Programers | Roseta\_S16 | 3 | Patch\_Panel\_S3 | 8 |
| SW\_P1-3 | g1/0/9 | 40 | Programers | Roseta\_S17 | 0 | Patch\_Panel\_S3 | 9 |
| SW\_P1-3 | g1/0/10 | 40 | Programers | Roseta\_S17 | 1 | Patch\_Panel\_S3 | 10 |
| SW\_P1-3 | g1/0/11 | 40 | Programers | Roseta\_S17 | 2 | Patch\_Panel\_S3 | 11 |
| SW\_P1-3 | g1/0/12 | 40 | Programers | Roseta\_S18 | 0 | Patch\_Panel\_S3 | 12 |
| SW\_P1-3 | g1/0/13 | 40 | Programers | Roseta\_S18 | 1 | Patch\_Panel\_S3 | 13 |
| SW\_P1-3 | g1/0/14 | 40 | Programers | Roseta\_S18 | 2 | Patch\_Panel\_S3 | 14 |
| SW\_P1-3 | g1/0/15 | 40 | Programers | Roseta\_S19 | 0 | Patch\_Panel\_S3 | 15 |
| SW\_P1-3 | g1/0/16 | 40 | Programers | Roseta\_S19 | 1 | Patch\_Panel\_S3 | 16 |
| SW\_P1-3 | g1/0/17 | 40 | Programers | Roseta\_S19 | 2 | Patch\_Panel\_S3 | 17 |
| SW\_P1-3 | g1/0/18 | 40 | Programers | Roseta\_S19 | 3 | Patch\_Panel\_S3 | 18 |
| SW\_P1-3 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/21 | 120 | Printers | Roseta\_S21 | 0 | Patch\_Panel\_S3 | 21 |
| SW\_P1-3 | g1/0/22 | 120 | Printers | Roseta\_S21 | 1 | Patch\_Panel\_S3 | 22 |
| SW\_P1-3 | g1/0/23 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/24 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/3 | N/A | N/A |
| SW\_P1-3 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/3 | N/A | N/A |
| SW\_P1-3 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/1 | 130 | Recepcion | Roseta\_B0 | 0 | Patch\_Panel\_B1 | 1 |
| SW\_P0-1 | g1/0/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/12 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/13 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/14 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/19 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/20 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/21 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/22 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/23 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/24 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/4 | N/A | N/A |
| SW\_P0-1 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/4 | N/A | N/A |
| SW\_P0-1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |

Tabla ‑ Conexionado Físico

1. Políticas de ciberseguridad Puestos de trabajo

A lo largo del siguiente anexo se describen las siguientes políticas en el puesto de trabajo:

* Contraseñas
* Escritorio limpio
* Uso de correo electrónico
* Actualizaciones
* Redes sociales
  1. Contraseñas
     1. Resumen

Las contraseñas son un aspecto muy importante cuando hablamos de proteger cuentas. Son la primera línea de defensa frente a el acceso no autorizado a las mismas. Desde Bionica Automations nos comprometemos a seleccionar contraseñas seguras para proteger nuestra red corporativa. Tanto empleados como proveedores que tengan acceso a las redes de Bionica Automations son responsables de tomas las medidas necesarias para escoger y securitizar sus contraseñas.

* + 1. Proposito

El propósito de esta política es establecer una serie de reglas para la creación de contraseñas seguras, su correcto almacenamiento y cada cuento tiempo deben cambiar.

* + 1. Audiencia

Esta política es aplicable a todo el personal de Bionica Automations que posea de una cuenta corporativa o cualquier tipo de acceso que requiera una contraseña para acceder a las instalaciones de Bionica Automations, para el acceso a las redes corporativas de Bionica Automations o gestiona información privada de Bionica Automations.

* + 1. Política
       1. Contraseñas de usuario

Todas las contraseñas de acceso a la red corporativa de Bionica Automations tiene n que cumplir los siguientes requisitos:

* Las contraseñas deben cambiar cada 90 días
* Las contraseñas deben tener un mínimo de 10 caracteres
* Las contraseñas deben contener una combinación de caracteres alfanuméricos y caracteres especiales cuando el sistema informático lo permita (!@#$%^&\*\_+=?/~’;’,<>|\).
* Las contraseñas no pueden estar relacionadas con la persona que las crea como puede ser el nombre de usuario, el número de la seguridad social, el DNI, un apodo, el cumpleaños, etc.
* Las contraseñas no pueden ser palabras del diccionario o acrónimos
* Las contraseñas no se pueden reutilizar en 1 año
  + - 1. Contraseñas de administradores

Todas las contraseñas de administradores tienen que seguir las siguientes reglas:

* La contraseña debe cambiar cada 6 meses
* La contraseña debe tener un mínimo de 12 caracteres y contener a menos tres de los siguientes tipos de caracteres: mayúsculas, minúsculas, números, caracteres especiales.
* Si hay contraseñas que nunca expiran deben estar documentadas y seguir los requisitos mencionados en el punto anterior
* Los administradores no pueden eludir la política de contraseñas en aras de la facilidad de uso
  + - 1. Protección de contraseñas
* No se debe usar la misma contraseña para múltiples cuentas.
* Nunca se deben compartir las contraseñas con nadie. Todas las contraseñas están catalogadas como información confidencial de Bionica Automations.
* Las contraseñas guardadas deben ser encriptadas
* Las contraseñas un deben ser escritas en correos electrónicos ni en otras formas de comunicación electrónica
* Las contraseñas nunca deben ser dichas o escritas por teléfono
* Las contraseñas nunca deben ser reveladas en cuestionarios o formularios de seguridad
* Las contraseñas de Bionica Automations nunca deben ser compartidas a nadie, incluso compañeros de trabajo, jefes, miembros de tu familia mientras estás de vacaciones.
* Las contraseñas nunca deben ser escritas en papel y almacenadas en la oficina de la empresa. Las contraseñas no pueden almacenar se en texto plano en dispositivos electrónicos
* Si la seguridad de una cuenta se ve comprometida hay que cambiar su contraseña de inmediato y avisar al soporte IT
* Nunca se debe habilitar (recordar contraseñas o similares) en paginas web ni hardcodear contraseñas en código a excepción de casos puntuales como por ejemplo backups automáticos
* Al abandonar el puesto de trabajo nunca se debe dejar el equipo desbloqueado, además de configurar un salvapantallas con contraseña.
* Cualquier tarjeta física, tokens RSA o método de autenticación deberá ser devuelto al terminar la relación laboral con Bionica Automations.

Escritorio Limpio

* + 1. Resumen

Bionica Automations se compromete a proteger la privacidad de sus empleados y miembros y también protegerá la confidencialidad de la información no pública de conformidad con las leyes estatales y federales.

Bionica Automations tiene la obligación de garantizar la seguridad y confidencialidad de los datos de miembros y de proteger estos datos contra el acceso no autorizado que podría resultar en cualquier tipo de pérdida o inconveniente para sus miembros.

* + 1. Propósito

El propósito y el principio de una política de "escritorio limpio" es garantizar que los datos confidenciales no estén expuestos a personas que puedan pasar por el área, como miembros, personal de servicio y ladrones. Fomenta la gestión metódica del espacio de trabajo.

Debido al riesgo de verse comprometida, la información confidencial siempre debe tratarse con cuidado.

* + 1. Política

Para mantener la seguridad y privacidad de la información personal de los empleados y miembros de Bionica Automations deben observar la regla de "escritorio limpio". Todos los empleados deben tomar las medidas apropiadas para evitar que personas no autorizadas tengan acceso a la información, las aplicaciones o los datos de los miembros. Los empleados también deben hacer una verificación concienzuda de su entorno de trabajo circundante para garantizar que no haya pérdida de confidencialidad en los medios de datos o documentos.

La política de escritorio limpio se aplica a:

* Planificadores de trabajo que puedan contener información confidencial
* Archivadores, armarios de almacenamiento y maletines que contienen información sensible o confidencial
* Cualquier dato confidencial o sensible, incluidos informes, listas o declaraciones. Los datos sensibles se refieren a la información personal y los datos restringidos. La información personal incluye, pero no se limita a:
  + Nombres individuales
  + Número de la seguridad social
  + Permiso de conducir
  + Número de cuenta
* Aparatos electrónicos, incluidos teléfonos móviles
* Llaves para acceder a información sensible
* Documentos que contengan información sensible
* Documentos en impresoras, fotocopiadoras y faxes
* El ordenador de trabajo y contraseñas
* Medios de almacenamiento externos como USBs, CDs

Uso del correo electrónico

* + 1. Resumen

El correo electrónico de Bionica Automations debe administrarse como un recurso valioso y de misión crítica. Así, esta política se establece para:

* Crear prácticas prudentes y aceptables con respecto al uso de los recursos de información
* Educar a las personas que pueden utilizar los recursos de información con respecto a sus responsabilidades asociadas con dicho uso
* Establezca un cronograma para retener y archivar el correo electrónico
  + 1. Propósito

El propósito de esta política es establecer reglas para el uso del correo electrónico de Bionica Automations para enviar, recibir o almacenar correo electrónico.

* + 1. Audiencia

Esta política se aplica por igual a todas las personas a las que se otorgan privilegios de acceso a cualquier recurso de información de Bionica Automations con capacidad para enviar, recibir o almacenar correo electrónico.

* + 1. Legal

Las personas involucradas pueden ser consideradas responsables de:

* Enviar o reenviar correos electrónicos con comentarios calumniosos, difamatorios, ofensivos, racistas u obscenos.
* Enviar o reenviar información confidencial sin permiso
* Enviar o reenviar material protegido por derechos de autor sin permiso
* Enviar o reenviar a sabiendas un archivo adjunto que contiene un virus
  + 1. Política

El correo electrónico corporativo no es privado. Los usuarios renuncian expresamente a cualquier derecho de privacidad en cualquier cosa que creen, almacenen, envíen o reciban en los sistemas informáticos de Bionica Automations. Bionica Automations puede, pero no está obligado a, monitorear los correos electrónicos sin notificación previa. Todos los correos electrónicos, archivos y documentos, incluidos los correos electrónicos, archivos y documentos personales, son propiedad de Bionica Automations, pueden estar sujetos a solicitudes de registros abiertos y se puede acceder a ellos de acuerdo con esta política.

El correo electrónico entrante debe tratarse con sumo cuidado debido a los riesgos inherentes a la seguridad de la información. Se utiliza una aplicación antivirus para identificar códigos o archivos maliciosos. Todo el correo electrónico está sujeto al filtrado entrante de archivos adjuntos de correo electrónico para buscar virus, códigos maliciosos o spam. El spam se pondrá en cuarentena para que el usuario lo revise para determinar su relevancia. La introducción de un virus o código malicioso en los sistemas de Bionica Automations podría causar estragos en la capacidad de realizar negocios. Si el escaneo automático detecta un riesgo de seguridad, se debe notificar inmediatamente al departamento de TI.

Se han iniciado prácticas contra la suplantación de identidad para detectar correos electrónicos falsificados. Los empleados deben ser diligentes en la identificación de un correo electrónico falsificado. Si se ha producido una suplantación de identidad por correo electrónico, se debe notificar inmediatamente al departamento de TI.

Los correos electrónicos entrantes se analizan en busca de archivos adjuntos maliciosos. Si se identifica que un archivo adjunto tiene una extensión que se sabe que está asociada con malware, o que es propenso al abuso por parte de malware o malos actores, o que presenta un mayor riesgo, el archivo adjunto se eliminará del correo electrónico antes de la entrega. El rechazo de correo electrónico se logra a través de la lista de dominios y direcciones IP asociadas con actores maliciosos. No se entregará ningún correo electrónico entrante procedente de un actor malicioso conocido. Cualquier cuenta de correo electrónico que se comporte mal al enviar spam se cerrará. Se realizará una revisión de la cuenta para determinar la causa de las acciones.

El correo electrónico debe usarse con fines comerciales y de manera coherente con otras formas de comunicación comercial profesional. Todos los archivos adjuntos salientes se analizan automáticamente en busca de virus y códigos maliciosos. La transmisión de un archivo adjunto dañino no solo puede dañar el sistema del destinatario, sino también dañar la reputación de Bionica Automations. Las siguientes actividades están prohibidas por la política:

Envío de correo electrónico que pueda considerarse intimidatorio, acosador u ofensivo. Esto incluye, pero no se limita a: lenguaje abusivo, comentarios o imágenes sexualmente explícitos, blasfemias, comentarios difamatorios o discriminatorios con respecto a la raza, credo, color, sexo, edad, religión, orientación sexual, origen nacional o discapacidad.

* Usar el correo electrónico para realizar negocios personales.
* Usar el correo electrónico con el fin de enviar SPAM u otras solicitudes no autorizadas.
* Violar las leyes de derechos de autor mediante la distribución ilegal de obras protegidas.
* Enviar correo electrónico utilizando la cuenta de correo electrónico de otra persona, excepto cuando esté autorizado a enviar mensajes para otra persona mientras se desempeña en una función de apoyo administrativo.
* Crear una identidad falsa para eludir la política.
* Falsificar o intentar falsificar mensajes de correo electrónico.
* Usar software de correo electrónico no autorizado.
* Deshabilitar a sabiendas el escaneo automático de archivos adjuntos en cualquier computadora personal de Bionica Automations.
* Eludir a sabiendas las medidas de seguridad del correo electrónico.
* Enviar o reenviar correos electrónicos de broma, cartas en cadena o cartas falsas.
* Envío de mensajes no solicitados a grupos grandes, excepto cuando sea necesario para realizar negocios de Bionica Automations.
* Envío de mensajes o archivos adjuntos excesivamente grandes.
* Enviar o reenviar a sabiendas correos electrónicos con virus informáticos.
* Configurar o responder en nombre de Bionica Automations sin la aprobación de la gerencia.

Todo el material confidencial o sensible de Bionica Automations transmitido por correo electrónico, fuera de la red de Bionica Automations, debe estar encriptado. Las contraseñas para descifrar los datos no deben enviarse por correo electrónico.

El correo electrónico no es seguro. Los usuarios no deben enviar por correo electrónico contraseñas, números de la seguridad social, números de cuenta, números PIN, fechas de nacimiento, apellido de soltera de la madre, etc. a terceros fuera de la red de Bionica Automations sin cifrar los datos. Toda la actividad de los usuarios en los activos del sistema de información de Bionica Automations está sujeta a registro y revisión. Bionica Automations cuenta con software y sistemas para controlar el uso del correo electrónico.

Los usuarios de correo electrónico no deben dar la impresión de que representan, dan opiniones o hacen declaraciones en nombre de Bionica Automations, a menos que estén debidamente autorizados (explícita o implícitamente) para hacerlo.

Los usuarios no deben enviar, reenviar ni recibir información confidencial o sensible de Bionica Automations a través de cuentas de correo electrónico que no sean de Bionica Automations. Los ejemplos de cuentas de correo electrónico que no son de Bionica Automations incluyen, entre otros, Hotmail, correo de Yahoo, correo de AOL y correo electrónico proporcionado por otros proveedores de servicios de Internet (ISP). Los usuarios con dispositivos móviles que no sean de Bionica Automations deben cumplir con la Política de seguridad y uso aceptable de dispositivos personales para enviar, reenviar, recibir o almacenar información confidencial o sensible de Bionica Automations.

* + 1. Uso incidental

El uso personal incidental del envío de correo electrónico está restringido a los usuarios aprobados por Bionica Automations; no se extiende a familiares u otros conocidos. Sin la aprobación previa de la gerencia, el uso incidental no debe generar costos directos para Bionica Automations. El uso incidental no debe interferir con el desempeño normal de las funciones laborales de un empleado.

No se pueden enviar ni recibir archivos o documentos que puedan causar responsabilidad legal o vergüenza para Bionica Automations. El almacenamiento de archivos y documentos personales dentro de los sistemas de TI de Bionica Automations debe ser nominal.

* + 1. Retención de correos

Los mensajes se conservan durante 36 meses. Los correos electrónicos con más de 36 meses de antigüedad están sujetos a una depuración automática.

Los correos electrónicos eliminados y archivados están sujetos a una depuración automática.

* + 1. Archivado de correos

Solo el propietario de un buzón y el administrador del sistema tienen acceso al archivo.

Los mensajes se eliminarán del archivo en línea 36 meses después de la fecha original de envío/recepción.

Actualizaciones

* + 1. Resumen

Las actualizaciones del software son uno de los puntos clave en cuanto a la seguridad informática. Desde Bionica Automations nos comprometemos a mantener actualizados nuestros equipos de trabajo para mejorar la seguridad de la red corporativa.

* + 1. Propósito

Concienciar a los trabajadores Bionica Automations sobre la importancia de mantener los sistemas actualizados.

* + 1. Audiencia

Esta política es aplicable a todo el personal de Bionica Automations que posea un equipo de trabajo o cualquier otro dispositivo electrónico con acceso a la red corporativa.

* + 1. Detalles de la política

Bionica Automations recomienda aplicar los últimos parches que salgan por lo menos una vez al mes.

Bionica Automations recomienda siempre tener actualizadas las aplicaciones de trabajo como pueden ser:

* El navegador web
* El cliente de correo electrónico
* El sistema operativo

Redes sociales

* + 1. Descripción

El uso de redes sociales externas (es decir, Facebook, LinkedIn, Twitter, YouTube, etc.) dentro de las organizaciones con fines comerciales está aumentando. Bionica Automations se enfrenta a la exposición de cierta cantidad de información que puede ser visible para los amigos de los amigos de las redes sociales. Si bien esta exposición es un mecanismo clave que impulsa el valor, también puede crear un conducto inapropiado para que la información pase entre contactos personales y comerciales. Las herramientas para establecer barreras entre las redes personales y privadas y las herramientas para administrar cuentas de forma centralizada apenas están comenzando a surgir. La participación del Departamento de TI en cuestiones de seguridad, privacidad y ancho de banda es de suma importancia.

* + 1. Propósito de las redes sociales
* **Crear una imagen positiva:** Bionica Automations puede usar las redes sociales para promover una imagen positiva. Si bien esto es particularmente importante para las organizaciones generalmente vulnerables a la prensa negativa o al descontento de los consumidores, también se puede usar para mejorar la imagen de Bionica Automations dentro de la comunidad.
* **Aumento de la participación mental:** las redes sociales pueden llegar a grandes audiencias a un costo monetario muy bajo, brindando a Bionica Automations otro medio para la promoción y el aumento de la conciencia de Bionica Automations.
* **Mejorar la satisfacción de los socios:** Los socios que reciben un servicio más oportuno y personal, en el medio que ellos prefieren, estarán más satisfechos.
* **Obtener información de los miembros:** las redes sociales se pueden usar para monitorear la opinión pública sobre Bionica Automations, sus productos y servicios, o sus competidores.
* **Aumentar la retención de miembros:** el uso de las redes sociales genera afinidad y lealtad, ya que los miembros se comprometen con un medio que prefieren: algo que Bionica Automations necesita ofrecer para seguir siendo competitivo.
* **Aumento de los ingresos:** uso de las redes sociales para crear aplicaciones de red personalizadas (también conocidas como complementos) para la promoción de productos o la integración con los servicios en línea de Bionica Automations.
* **Adquisición de miembros:** Uso de las redes sociales para responder rápida y eficientemente a los problemas de servicio a los miembros. La respuesta al problema puede ser pública, lo que permite que otros miembros que tengan la misma solicitud puedan buscarla.
* **Recuperación ante desastres:** uso de las redes sociales para eliminar temores de manera rápida y eficiente y comunicar información precisa sobre las acciones de recuperación en caso de un desastre.
  + 1. política

Bionica Automations fomenta el uso de las redes sociales como un canal para la comunicación comercial, de acuerdo con la estrategia de comunicación y marketing corporativo de BCHHU. Es política de Bionica Automations establecer pautas para el uso seguro de las redes sociales con respecto a la protección de la información de Bionica Automations. La seguridad y confidencialidad de la información es vital para el éxito de Bionica Automations. Bionica Automations ha establecido esta política para establecer parámetros y controles relacionados con el uso de sitios web de redes sociales por parte de Bionica Automations.

* + - 1. Términos y condiciones de uso

Todas las solicitudes para el uso de redes sociales externas por parte de un empleado de Bionica Automations, en nombre de Bionica Automations, deben enviarse al Equipo Directivo Superior. Bionica Automations puede permitir el acceso a determinados sitios web de redes sociales preaprobados. Los funcionarios de Bionica Automations solo pueden acceder a estos sitios de una manera consistente con los protocolos de seguridad de Bionica Automations y los funcionarios de Bionica Automations no pueden eludir los protocolos de seguridad de TI para acceder a los sitios de redes sociales.

* + - 1. Está prohibido el uso de cuentas personales de redes sociales e identificaciones de usuario para Bionica Automations.

Se prohíbe el uso de ID de usuario de redes sociales de Bionica Automations para uso personal. Está prohibido el uso de las direcciones de correo electrónico de Bionica Automations para registrarse en redes sociales, blogs u otras herramientas en línea utilizadas para uso personal. Los ejemplos de uso prohibido de las identificaciones de usuario de la empresa incluyen:

* Descargar e instalar complementos o aplicaciones auxiliares, como las que intentan acceder al directorio de correo electrónico de Bionica Automations
* Unirse a grupos utilizando una identificación de usuario de la empresa por motivos personales
* Agregar amigos personales a la lista de amigos de un oficial de Bionica Automations
* Los funcionarios de Bionica Automations deben reconocer que han revisado los Términos de servicio o los Términos de usuario del servicio de redes sociales, según corresponda. Los enlaces para los sitios están abajo.
  + - 1. Representando a Bionica Automations

La alta gerencia de Bionica Automations designará a una persona o equipo para administrar y responder a los problemas de las redes sociales relacionados con Bionica Automations y determinará quién tendrá la autoridad para contribuir con el contenido. Las responsabilidades de esta(s) persona(s) incluirán, pero no se limitarán a:

* **Gestión** de herramientas y canales de redes sociales;
* **Responder** a preguntas internas y externas sobre el sitio de redes sociales;
* **Abordar** problemas/brindar orientación al personal si un usuario se vuelve amenazante, abusivo o acosador;
* **Sugerir** cambios a esta política de medios sociales de Bionica Automations cuando se justifique;
* **Trabajar** con otros miembros del personal para asegurarse de que no se pasen por alto las oportunidades en la comercialización de los servicios de Bionica Automations; y
* **Capacitar** al personal para garantizar que entiendan cómo usar el programa de redes sociales de Bionica Automations.

Bionica Automations tomará las medidas necesarias para asegurarse de que el contenido cumpla con las leyes y regulaciones aplicables.

Se espera que todos los empleados de Bionica Automations que participan en las redes sociales, en nombre de Bionica Automations, representen a Bionica Automations de manera profesional. De lo contrario, podría tener un impacto negativo en Bionica Automations y podría poner en peligro la capacidad de un empleado de Bionica Automations para participar en las redes sociales en el futuro.

Bionica Automations es propietaria de todo el contenido de redes sociales y redes sociales autorizado. Los funcionarios de Bionica Automations tienen prohibido tomar, guardar o enviar cualquier contenido de Bionica Automations distribuido a través de las redes sociales mientras estén empleados, separados, sirviendo en la Junta Directiva o despedidos por Bionica Automations.

Las nuevas tecnologías y herramientas de redes sociales evolucionan continuamente. A medida que surjan nuevas herramientas, esta política se actualizará para reflejar los cambios.

Las plataformas para la colaboración en línea están cambiando fundamentalmente el entorno de trabajo y ofrecen nuevas formas de interactuar con los miembros y la comunidad. Se deben seguir los principios rectores para participar en las redes sociales.

* Publique comentarios significativos y respetuosos y absténgase de hacer comentarios fuera de tema u ofensivos.
* Responda a los comentarios rápidamente cuando la respuesta sea adecuada.
* Conozca y siga las leyes estatales y federales que protegen la confidencialidad de los miembros en todo momento.
* Proteger la información de propiedad exclusiva y la confidencialidad.
* Cuando no esté de acuerdo con las opiniones de los demás, manténgalo profesional.
* Conocer el Código de Conducta de Bionica Automations y aplicar los estándares y principios en computación social.
  + - 1. Blogs personales y posts

Bionica Automations no se pronuncia sobre la decisión de un empleado de Bionica Automations de iniciar o mantener un blog o sitio web personal o de participar en otras actividades de redes sociales en línea fuera del trabajo. Los funcionarios de Bionica Automations, que se identifican como funcionarios de Bionica Automations en una red social, deben asegurarse de que su perfil y el contenido relacionado sean coherentes con la forma en que ellos y Bionica Automations desean que se presenten. Esto incluye lo que el empleado de Bionica Automations escribe sobre sí mismo y el tipo de fotos que publica.

Los funcionarios de Bionica Automations no deben revelar información patentada y deben tener cuidado con la publicación de exageraciones, obscenidades u otras caracterizaciones que puedan provocar litigios.

Los funcionarios de Bionica Automations no deben hacer referencia pública a ningún procedimiento de seguridad o efectivo relacionado con Bionica Automations.

Los funcionarios de Bionica Automations que comenten sobre cualquier problema comercial o de política de Bionica Automations deben identificarse claramente como funcionarios de Bionica Automations en su blog o publicación e incluir un descargo de responsabilidad de que las opiniones son propias y no de Bionica Automations. Al generar contenido relacionado con Bionica Automations o personas asociadas con Bionica Automations, los funcionarios de Bionica Automations deben usar un descargo de responsabilidad como "Las publicaciones en este sitio son mías y no necesariamente reflejan las opiniones de Bionica Automations".

Los funcionarios de Bionica Automations no deben utilizar los sitios web de redes sociales para acosar, amenazar, discriminar, menospreciar o difamar a cualquier otro funcionario, miembro, proveedor, producto, servicio o filosofía comercial de Bionica Automations.

Los empleados de Bionica Automations tienen prohibido divulgar información comercial o personal confidencial, patentada o confidencial relacionada con Bionica Automations o cualquiera de sus empleados, proveedores o miembros de Bionica Automations. Los funcionarios de Bionica Automations también tienen prohibido divulgar cualquier información comercial o personal confidencial, patentada o sensible que pueda identificar a otro funcionario, proveedor o miembro de Bionica Automations sin la autorización previa de esa persona.

Los empleados de Bionica Automations no deben realizar ninguna acción a través de sitios web de redes sociales o blogs personales que puedan dañar, o puedan dañar, la reputación de Bionica Automations o cualquier empleados, miembro o proveedor de Bionica Automations.

* + - 1. Reglas de escritura
* Los funcionarios de Bionica Automations deben escribir y publicar sobre sus áreas de especialización, especialmente en lo que se refiere a Bionica Automations.
* Escribe en primera persona. Hable con el lector como si fuera una persona real en una situación profesional.
* Evite un lenguaje demasiado compuesto.
* Considere el contenido que es abierto e invita a la respuesta.
* Fomente los comentarios.
* Utilice un corrector ortográfico.
* Haga el esfuerzo de ser claro, completo y conciso en la comunicación. Determine si el material se puede acortar o mejorar.
* Si se comete un error, debe reconocerse. Sea sincero y sea rápido con la corrección. Si publica en un blog, aclare si se ha realizado una modificación en una publicación anterior.

Produce material que los miembros de Bionica Automations valorarán. La comunicación en las redes sociales de Bionica Automations debería ayudar a sus miembros, socios y compañeros de trabajo. se debe pensar

provocando y construyendo un sentido de comunidad. Debería ayudar a los miembros a mejorar su conocimiento o comprender mejor a Bionica Automations o a un afiliado.

El contenido anónimo no está permitido en los sitios de Bionica Automations.

* + - 1. Uso personal de sitios de terceros durante el horario laboral

El correo electrónico y el acceso a Internet se proporcionan para respaldar los fines comerciales de Bionica Automations. Si se accede a estas herramientas, se permite el uso personal incidental de las mismas. En general, Bionica Automations limitará el acceso a los sitios de redes sociales a los funcionarios de Bionica Automations que lo usan en nombre de Bionica Automations. No se permite el uso personal excesivo de cualquier herramienta de Internet durante el tiempo de trabajo y los privilegios de acceso pueden ser revocados por abuso del sistema.

* + - 1. Las represalias están prohibidas

Bionica Automations prohíbe tomar medidas negativas contra cualquier funcionario de Bionica Automations por informar una posible desviación de esta política o por cooperar en una investigación. Cualquier funcionario de Bionica Automations que tome represalias contra otro funcionario de Bionica Automations por informar una posible desviación de esta política o por cooperar en una investigación estará sujeto a medidas disciplinarias, que pueden incluir el despido en Bionica Automations o remoción de la Junta Directiva.

1. Pulseway
   1. Administración de dispositivos

Dentro de este apartado se engloba todas las funcionalidades que tienen que ver con la administración IT de activos:

* + 1. Descubrimiento y despliegue

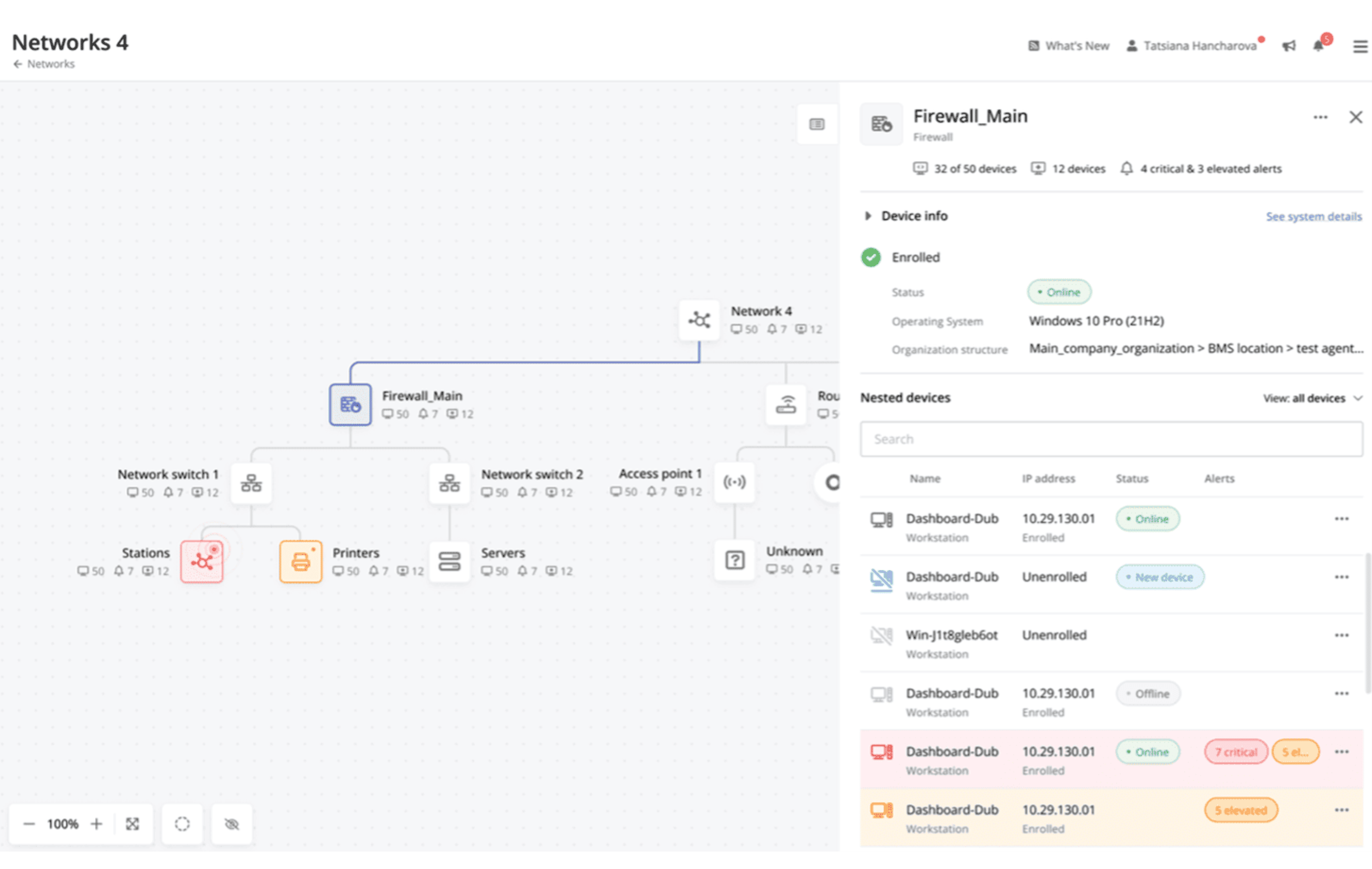


Figura ‑ Pulseway endpoint discovery

En minutos, verá rápidamente todos los endpoints se muestran en la herramienta. A continuación, puede implementar fácilmente Pulseway en masa con políticas preconfiguradas integradas. Comience rápidamente a dar soporte a sus clientes sin la necesidad de una incorporación o capacitación costosa y que consume mucho tiempo.

* + 1. Monitorización y administración

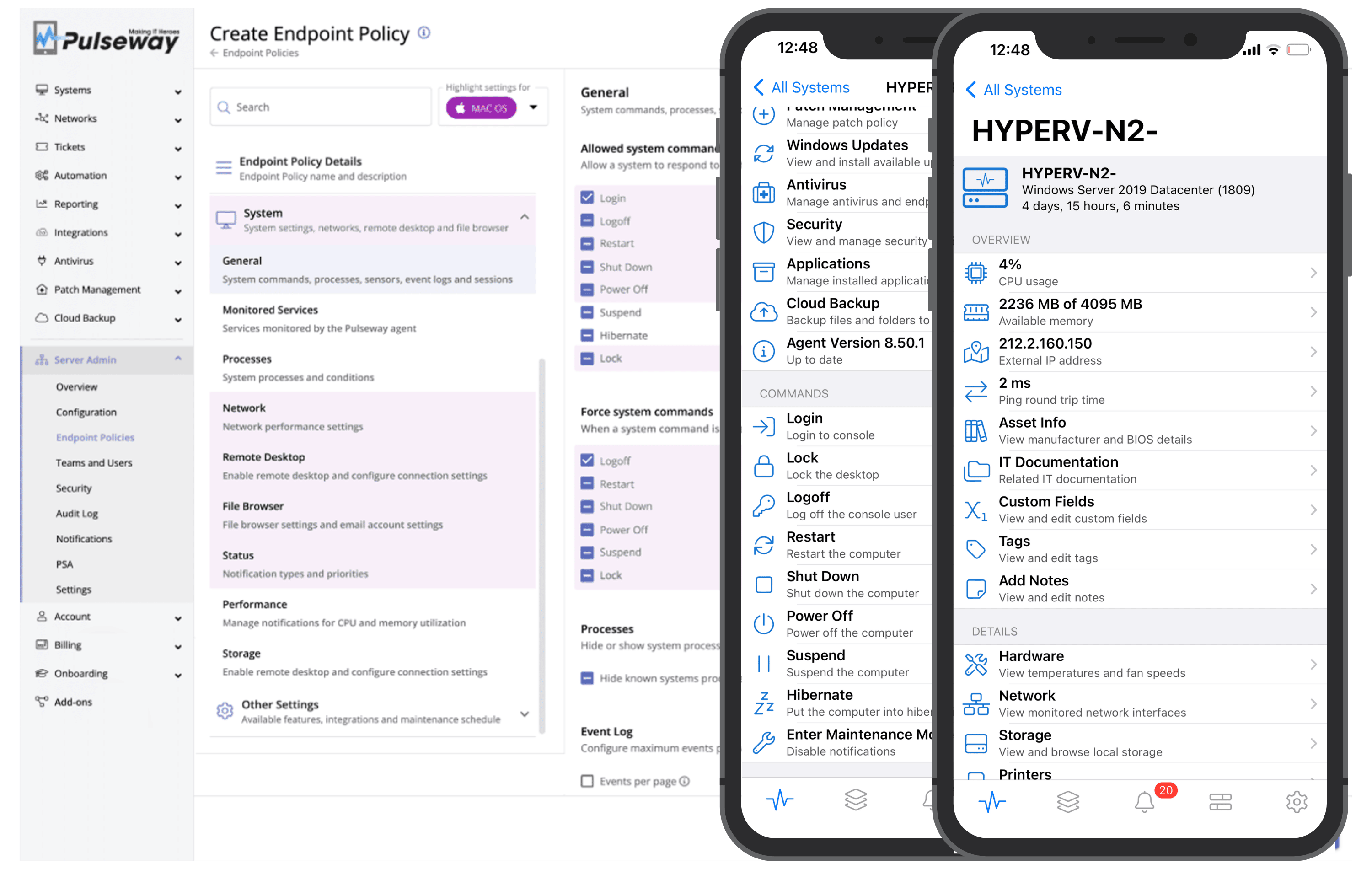


Figura ‑ Monitorización y Administración

La interfaz intuitiva de Pulseway significa que cualquier técnico puede ser productivo instantáneamente con información detallada, procesable y en tiempo real en servidores, estaciones de trabajo y dispositivos de red. Combinado con alertas personalizables, puede identificar rápidamente problemas, comunicarse con los clientes y resolver problemas con comandos y scripts integrados, incluso desde su dispositivo móvil.

Desea ofrecer el mismo nivel de servicio a todos sus clientes y con la aplicación de administración de TI móvil más rica en funciones de la industria, puede hacerlo. Su equipo ahora puede hacer su trabajo desde cualquier lugar para que puedan responder rápidamente a cualquier problema, de cualquier cliente, directamente desde sus teléfonos inteligentes.

* + 1. Automatización y auto remediación



Figura ‑ Automatizaciones

Haga más haciendo menos, con el potente motor de automatización de Pulseway. Al combinar la tecnología de flujo de trabajo con una interfaz de usuario intuitiva, puede configurar activadores inteligentes para solucionar automáticamente los problemas de TI de inmediato antes de que tengan la oportunidad de convertirse en un problema, lo que le ayuda a cumplir o superar sus SLA. Puede ahorrar aún más el valioso tiempo de su equipo automatizando tareas repetitivas y cotidianas utilizando nuestra amplia biblioteca de scripts integrados, plantillas y automatización específica de funciones, liberándolos para centrarse en actividades de mayor valor.

* + 1. Administración de parches de seguridad

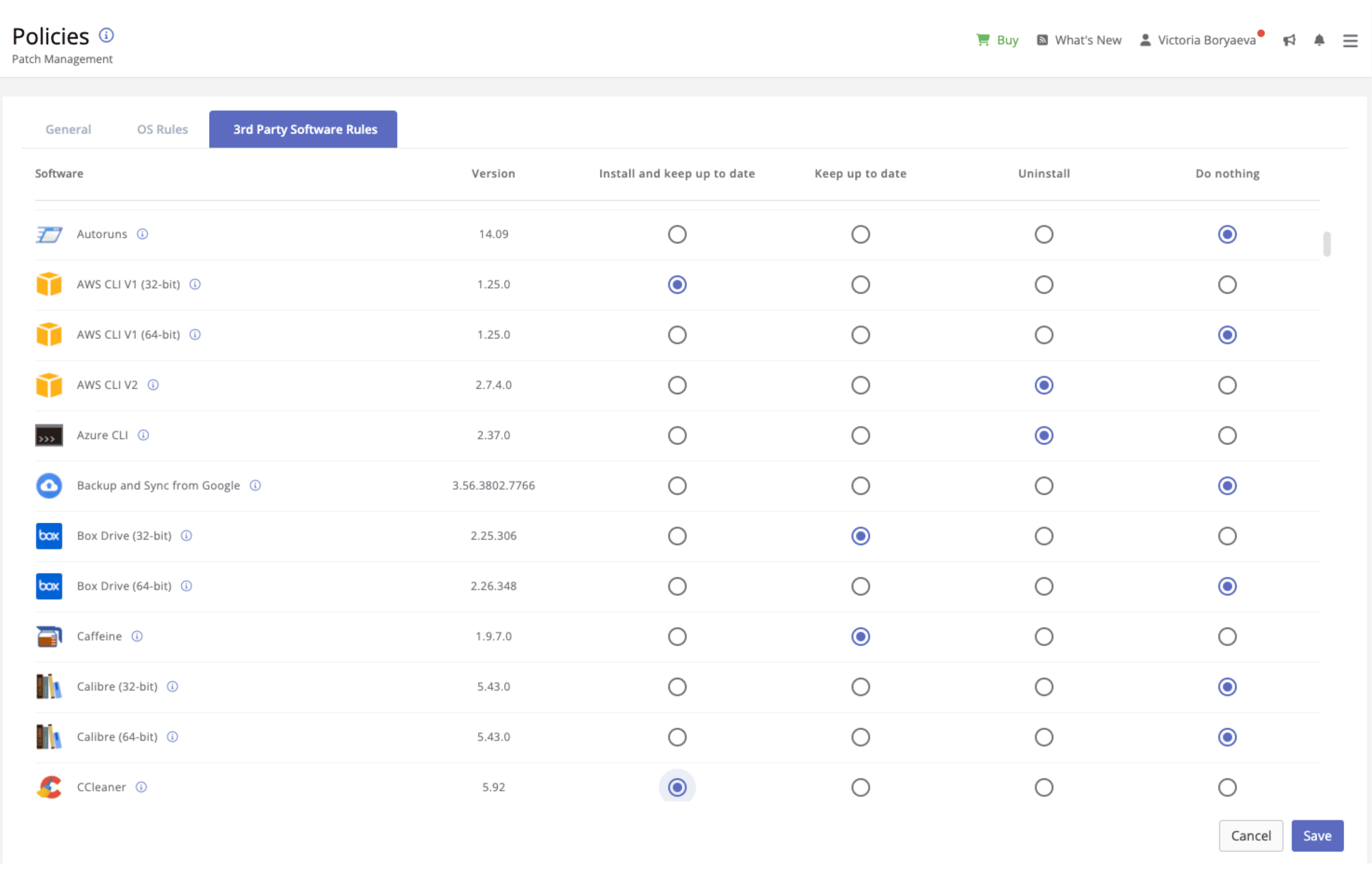


Figura ‑ Parches de Seguridad

La administración de parches puede ser una pérdida de tiempo y recursos a medida que intenta mantenerse al tanto de la aplicación de parches en todos sus clientes, especialmente cuando intenta garantizar que se prioricen los críticos. El potente software de administración de parches de Pulseway automatiza el descubrimiento y la aplicación de parches de aplicaciones de terceros y sistemas operativos. Las políticas de parches integrales le permiten definir el qué, dónde y cuándo de la aplicación de parches por adelantado. Más de 220 aplicaciones de terceros de uso común son compatibles de fábrica, pero puede agregar fácilmente aplicaciones especializadas con nuestra función de aplicaciones personalizadas para garantizar que todas sus aplicaciones se mantengan actualizadas.

* + 1. Detección de Ransomware y AV integrado

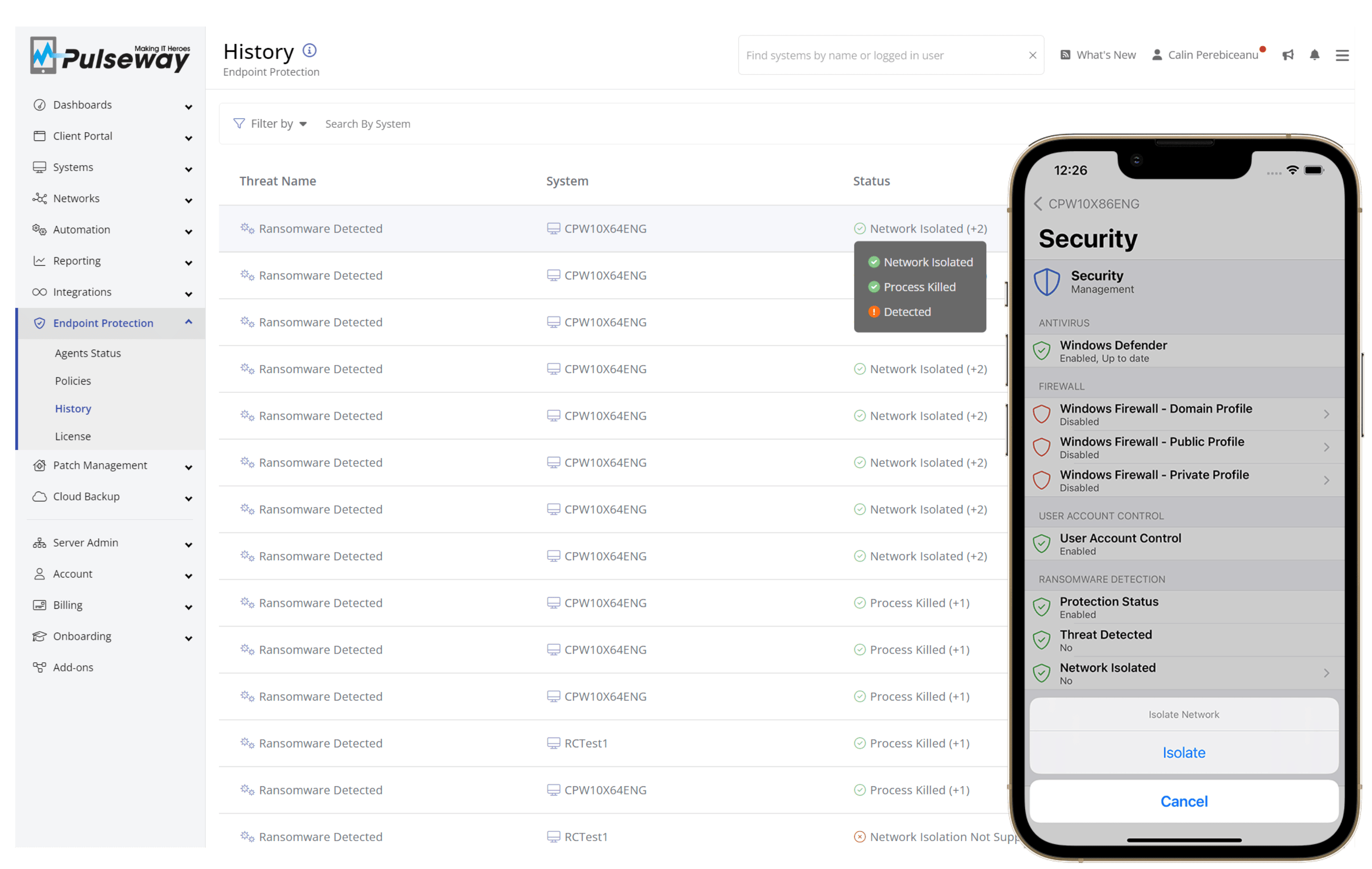


Figura ‑ Detección de Ransomware

Supervise, detecte, detenga y elimine de forma proactiva la actividad de ransomware en dispositivos Windows administrados con Pulseway Ransomware Detection integrado de forma nativa en los agentes de Pulseway. Además, la solución AV integrada de Pulseway le permite administrar Bitdefender o Webroot directamente desde la consola RMM. Además de simplificar la implementación, también habilitamos la inscripción automática para que cualquier dispositivo nuevo agregado a la red se inscriba automáticamente en el AV.

* 1. Backup & Disaster Recovery

El sistema de copias de seguridad que posee Pulseway esta desarrollada por Unitrends y es capaz de hacer copias de seguridad de entornos SaaS como Microsoft 365, Google Workspace o Salesforce.

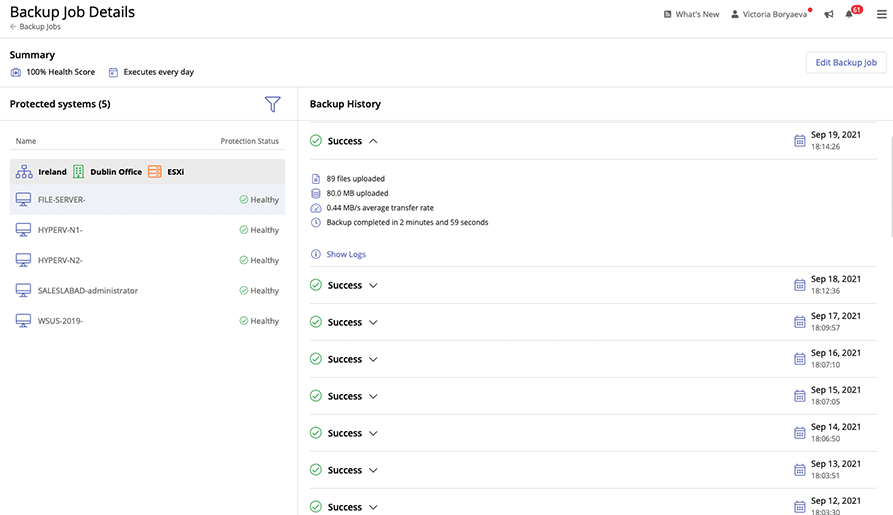


Figura ‑ Backup & Disaster Recovery

Muchos usuarios de estas plataformas no se dan cuenta de que no están protegidos contra la pérdida de datos causada por una acción accidental o maliciosa del usuario, y necesitan hacer sus propios arreglos de copia de seguridad.

* 1. Protección contra Ransomware

Pulseway posee características esenciales para detectar, prevenir y remediar cualquier incidente de Ransomware.

Además, incluye planes de concienciación para los empleados de la compañía para evitar el Phishing, además de incluir una protección ante este tipo de ataques.

* + 1. Protección contra Phishing

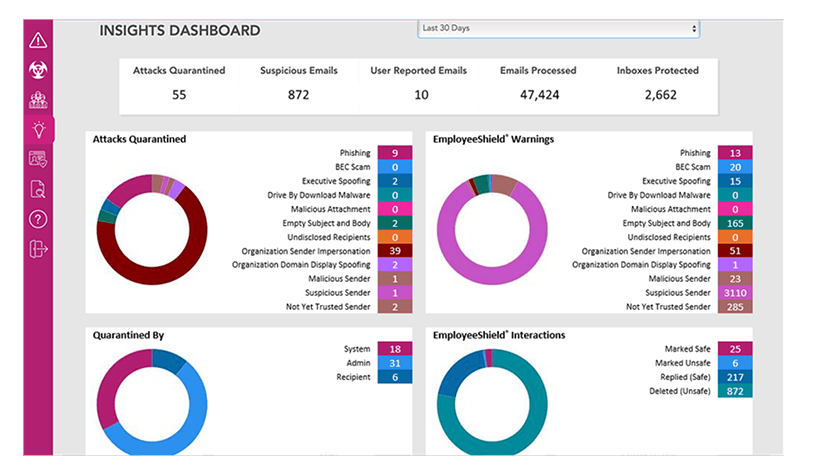


Figura ‑ Phishing

**El 91% de todos los ataques cibernéticos comienzan a partir de correos electrónicos de phishing** Pulseway combate eso con una solución basada en la nube que detecta y bloquea el 99.9% de los ataques sofisticados de correo electrónico antes de que lleguen a las bandejas de entrada de los empleados.

* Analizar las relaciones comerciales de sus empleados (con quién trabajan, con qué frecuencia se comunican, etc.) para crear perfiles de confianza.
* Analizar en busca de irregularidades sospechosas en el contenido y los archivos adjuntos de los mensajes y compararlos con perfiles de confianza para detectar ataques.
* Aprender de la interacción y los comentarios del usuario para crecer de manera más inteligente y defenderlo mejor de las nuevas amenazas emergentes.
  + 1. Planes de concienciación

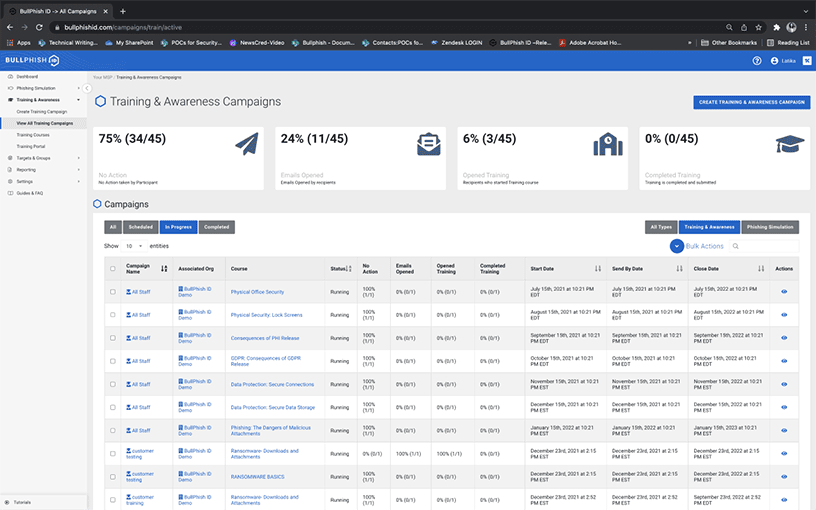


Figura ‑ Planes de concienciación

**El 90% de las violaciones de datos comienzan con un correo electrónico de phishing.** Reduzca las posibilidades de su organización de experimentar un desastre de ciberseguridad hasta en un 70% con capacitación en concientización sobre seguridad que incluye simulación de phishing.

* Agregue a todos los empleados a su equipo de seguridad con capacitación en concientización sobre seguridad que les permite detectar y detener las amenazas de phishing.
* Automatice las campañas de capacitación y los informes para obtener una capacitación consistente y sin estrés que obtenga resultados.
* Elija entre un amplio conjunto de kits de campaña anti-phishing plug-and-play.
  + 1. Escáner de vulnerabilidades

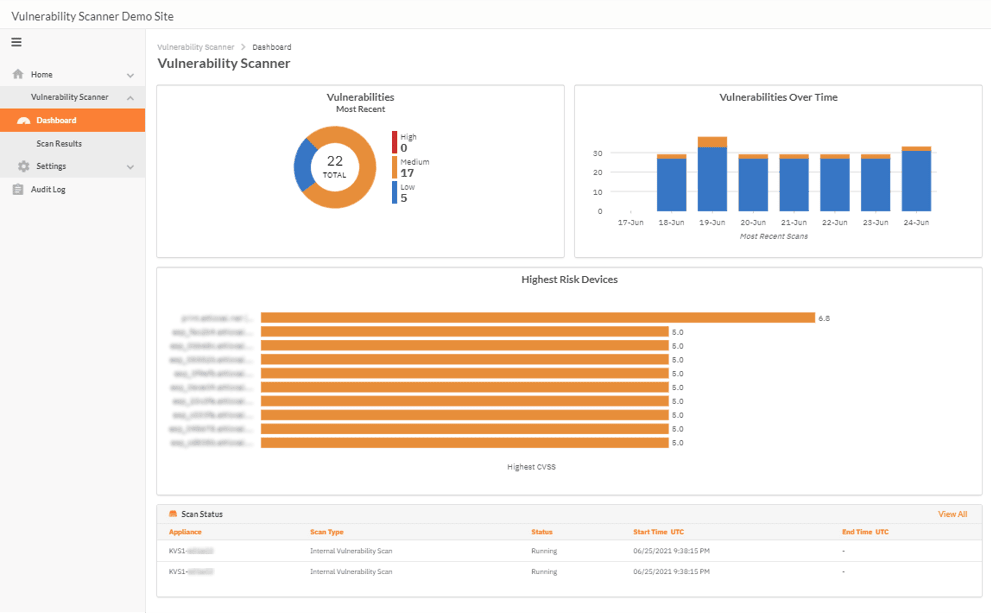


Figura ‑ Escáner de vulnerabilidades

El escáner de vulnerabilidades de Pulseway es un escáner de vulnerabilidades **automatizado y asequible que le alerta sobre vulnerabilidades en tiempo real.** Ofrece escaneo de vulnerabilidades internas y externas. Es fácil de usar y significa que cualquier organización ahora puede realizar fácilmente los escaneos de vulnerabilidad regulares que se consideran las mejores prácticas internacionales.

* + 1. Backup and Disaster Recovery

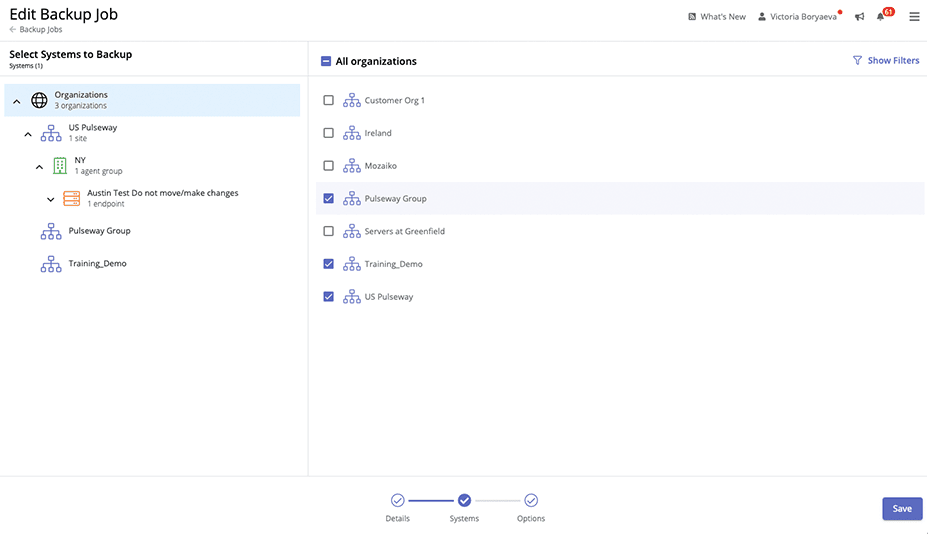


Figura ‑ Backup & Disaster Recovery

**Elimine la pérdida de datos y el tiempo de inactividad del ransomware** con detección integrada, protecciones de inmutabilidad y automatización que permite una recuperación rápida después de un ataque. Los datos viven en más lugares que nunca y están bajo ataque constante. Las copias de seguridad se encuentran entre las defensas más importantes contra el ransomware. Ahora es el momento de construir su plan de recuperación de ransomware para lograr la resiliencia cibernética.

# GLOSARIO

* ABREVIATURAS Y ACRÓNIMOS

| **Referencia** | **Descripción** |
| --- | --- |
| XDR | Extended Detection and Response |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| VPN | Virtual Private Network |
| VLAN | Virtual Local Area Network |
| IPS | Intrusion Prevention System |
| ACL | Access Control List |

* DEFINICIONES

| Referencia | Definición |
| --- | --- |
| VLAN | Red virtual |
| Active Directory | Para gestionar usuarios en entornos empresariales |
| DHCP | Servicio para proveer de configuración de red a los dispositivos |
| IPS | Es una aplicación que ayuda a las organizaciones a identificar el tráfico malicioso y bloquea de manera proactiva |
| XDR | Es una herramienta SaaS que ofrece seguridad holística y optimizada integrando productos de seguridad y datos en soluciones simplificadas |

# CONTROL DE CAMBIOS

| **Edición** | **Fecha** | **Descripción** | **Colaboradores** | |
| --- | --- | --- | --- | --- |
| **Elaborado** | **Revisado** |
| 01.00 | 2023-03-09 | Primera edición | D. Ubalde |  |