Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Estructura Lógica



[1 Glosario 3](#_Toc127389916)

[2 Introducción 4](#_Toc127389917)

[3 Ubicación del proyecto 6](#_Toc127389918)

[4 Justificaciones técnicas 7](#_Toc127389919)

[4.1 Tipos de medios de transmisión 7](#_Toc127389920)

[4.2 Elementos de la estructura física 7](#_Toc127389921)

[4.3 Estructura lógica 8](#_Toc127389922)

[4.4 Electrónica de red 8](#_Toc127389923)

[4.5 Ubicación del CPD 11](#_Toc127389924)

[5 Desarrollo del proyecto 12](#_Toc127389925)

[5.1 Estructura física y cableado estructurado 12](#_Toc127389926)

[5.1.1 Tipos de medios de transmisión 12](#_Toc127389927)

[5.1.2 Tomas de red 12](#_Toc127389928)

[5.1.3 Armarios de distribución o racks y pasacables 12](#_Toc127389929)

[5.1.4 Pach-panels 12](#_Toc127389930)

[5.1.5 Cableado horizontal 12](#_Toc127389931)

[5.1.6 Cableado vertical 12](#_Toc127389932)

[5.2 Estructura lógica 13](#_Toc127389933)

[5.2.1 Topología de red 13](#_Toc127389934)

[5.2.2 Diseño de la red 13](#_Toc127389935)

[5.2.3 Tipo de protocolo IP 13](#_Toc127389936)

[5.2.4 Direccionamiento IP y subredes 13](#_Toc127389937)

[5.3 Administración de servidores 13](#_Toc127389938)

[5.3.1 Sistemas operativos y software 13](#_Toc127389939)

[5.3.2 Servicios en red 14](#_Toc127389940)

[5.3.3 Active Directory - Usuarios y Grupos 14](#_Toc127389941)

[5.3.4 Active Directory – Recursos compartidos y cuotas de disco 14](#_Toc127389942)

[5.3.5 Sistemas de seguridad 14](#_Toc127389943)

[5.3.6 Directivas de grupo 15](#_Toc127389944)

[5.4 Administración de clientes 15](#_Toc127389945)

[5.4.1 Acceso clientes 15](#_Toc127389946)

[5.4.2 Sistemas de seguridad 15](#_Toc127389947)

[5.5 Ciberseguridad 16](#_Toc127389948)

[5.5.1 Inventario de Activos 16](#_Toc127389949)

[5.5.2 Firewall 27](#_Toc127389950)

[5.5.3 Switches 27](#_Toc127389951)

[5.5.4 Antivirus 27](#_Toc127389952)

[5.5.5 Directivas de seguridad 27](#_Toc127389953)

[5.5.6 Copias de seguridad 28](#_Toc127389954)

[5.5.7 Puesto de trabajo 28](#_Toc127389955)

[Anexo 1 - Diagrama Packet tracer 29](#_Toc127389956)

[Anexo 2 - Esquema de conexiones 29](#_Toc127389957)

[Anexo 3 – Plan de ciberseguridad 29](#_Toc127389958)

[Anexo 3 – Plan de ciberseguridad 29](#_Toc127389959)

# Glosario

|  |  |
| --- | --- |
| VLAN | Red virtual |
| Active Directory | Para gestionar usuarios en entornos empresariales |
| CPD | Armario centrar para los dispositivos de red (Rack) |
| DHCP | Servicio para proveer de configuración de red a los dispositivos |
| HSRP | [Hot Standby Routing Protocol](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-hot-standby-router-protocol.html) |
| DNS | Servidor de nombres de dominio |

# Introducción

Todas las grandes empresas dedicadas al sector informático tienen una serie de características en común que las hace diferentes unas de otras tales como, el esfuerzo por ofrecer un producto superior a la competencia, tener una buena plataforma fácil de usar donde vender sus productos, además de tener en cuenta la satisfacción del cliente y sus valoraciones para poder mejorar y, por último, el soporte que ofrecen a sus clientes cuando tienen problemas con sus productos.

Todo esto hace una imagen de la empresa solida de cara al público.

Las cualidades de nuestro sector informático van desde resolver problemas complejos a clientes, al desarrollo e implementación de nuevos productos.

Estas son algunas empresas del sector Informático en Zaragoza:

|  |  |
| --- | --- |
| EMPRESA | DEDICACIÓN |
| Informática Madi S L | Empresa de software |
| Ecomputer | Tienda de informática |
| Tecnovalia informática | Soporte y servicios |
| Tempus Informática, S.L. | Empresa de software |
| Implementación Informática Lyra | Consultoría |
| Informática Zaragoza | Soporte y servicios |
| Calat Sistemas y Comunicaciones S.L. | informática para empresas |
| DSI S.L. | Consultora |
| Izquierdo Informática S.L. | Soporte y servicios |
| SUIN | Soporte y servicios |
| Informática Torrero S.L. | Soporte y servicios |
| APP Informática | Soporte y servicios |
| Programas Y Sistemas informáticos S.L. | Soporte y servicios |
| Formación Y Desarrollo de Software Aplicado SL | Empresa de software |

El nombre de la empresa sobre la que vamos a trabajar es Bionica Automations.

Los productos que se van a vender y desarrollar van a ser productos de IoT, teles como enchufes inteligentes, luce, persiana, cerraduras, sistemas de climatización, monitorización de consumo eléctrico, etc….

He optado orientar la empresa en productos de IoT porque es un mercado emergente que tiene mucho que ofrecer, ya que de aquí a porco tiempo se van a empezar a implementar sistemas de domótica que se basan en IoT y en ese campo queremos ganar nuestro nicho de mercado.

# Ubicación del proyecto

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 siguientes departamentos:

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

# Justificaciones técnicas

## Tipos de medios de transmisión

Los medios de transmisión escogidos para el proyecto han sido: fibra óptica para las comunicaciones entre los dispositivos del CPD y el cableado vertical, cable de par trenzado para el cableado horizontal y el aire (WiFi).

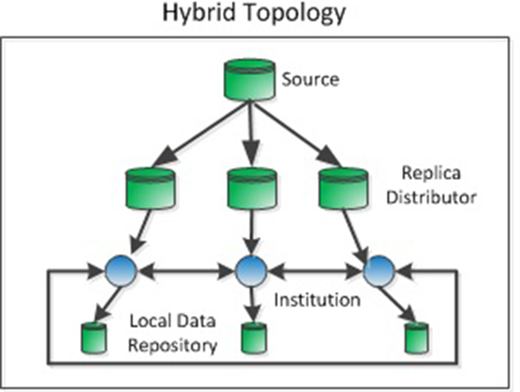
## Elementos de la estructura física

Pequeña tabla con algunos de los elementos que componen la estructura física de Bionica Automations.



## Estructura lógica

La topología de la red es una topología mixta o híbrida.

Existe una VLAN por departamento con su propio direccionamiento y servidor DHCP, el acceso a internet está garantizado gracias a dos Reuters configurados con el protocolo HSRP, también hay redundancia en el primer salto, todas las bocas que no están en uso están deshabilitadas y asignadas a una VLAN donde no hay nada, para maximizar la seguridad.

Los departamentos que lo necesiten tendrán disponibles en su subred los servicios necesarios para desempeñar su trabajo, como las impresoras en cado de los comerciales o contabilidad o también un NAS para los programadores y desarrolladores.

Para más información consultar el ANEXO 1 y 2

## Electrónica de red

Routers: Unifi Dream Machine Pro

Switches: Switch Pro 48 PoE y Switch Pro 48 PoE

Servidores: Dell PowerEdge XR12

NAS: Storinator Q30 Enhanced

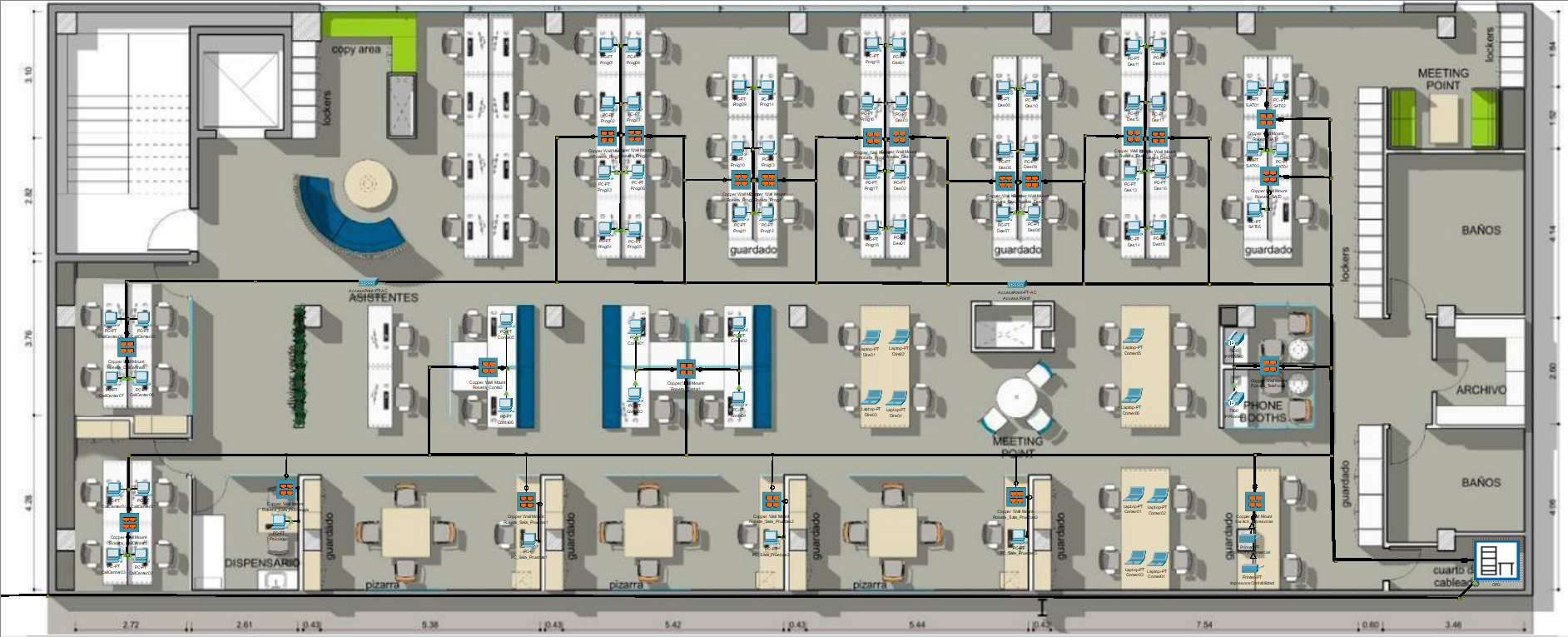
Todos los monitores salvo los de recepción van con soporte vesa.

|  |  |  |
| --- | --- | --- |
| Departamento | Ordenador | Periféricos |
| Recepción | Dell OptiPlex 3070 Micro Form Factor Config. Base | Monitor Dell 22 | P2219H  Teclado y ratón inalámbricos Dell | KM636 |
| Programadores | Dell Vostro Desktop 3670 MT  Intel® Core™ i5-8400  16 GB RAM | Conjunto de teclado y ratón inalámbricos KM636  X2 Monitor Dell 24 P2419H |
| I+D | Dell Vostro Desktop 3670 MT  Intel® Core™ i5-8400  16 GB RAM | X2 Monitor Dell 24 P2419H  Conjunto de teclado y ratón inalámbricos KM636 |
| Dirección | Portátil XPS 13  Intel® Core™ i5  8 GB RAM | Opcional: Ratón inalámbrico Dell Premier WM527 |
| Comercial | Dell 2 en 1 XPS de 13  Intel® Core™ i5  8 GB RAM | Opcional: Ratón inalámbrico Dell Premier WM527 |
| Contabilidad | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  8 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |

|  |  |  |
| --- | --- | --- |
| CallCenter | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  8 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636  Auriculares estéreo Dell Pro UC350 |
| Salas de pruebas | Dell Embedded Box PC 5000 | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |
| Informática | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  8 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |

## Ubicación del CPD

El CPD está situado en el cuarto del cableado eléctrico.



# Desarrollo del proyecto

## 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.

### Tomas de red

Las rosetas van acordes al número máximo de ordenadores que se pueden colocar en los puestos de trabajo cercanos.

Ejemplo: si se pueden colocar 8 ordenadores en un área de trabajo, se pondrán 4 rosetas de 2 bocas cada una para esos supuestos 8 ordenadores. Si solo se puede colocar 1 ordenador, en ese caso se pondrán rosetas individuales.

### 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-7 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 es una topología mixta porque integramos la estructura en árbol y en estrella a la vez.

### Diseño de la red

La red está formada por 2 routers conectados a 2 switches que están conectados entre ellos para garantizar la redundancia del primer salto, ambos routers están configurados en fail over, para que así si se interrumpe el servicio de alguno de los 2, el otro asuma la carga.

Luego tenemos los switches de cada plata conectados con los switches principales por fibra plástica de 10 Gb, con sus respectivos paneles de parcheo de RJ45 de CAT-7 conectado a las rosetas de las plantas, y estas a los dispositivos finales.

Los servidores están conectados a un switch central a través de cables CAT-7 RJ45.

Todas las conexiones con los equipos de trabajo se realizan bajo cable de par trenzado CAT-7 de 1Gb, las rosetas por supuesto son CAT-7 también.

### Tipo de protocolo IP

Solo se implementa el protocolo IPv4 ya que como máximo vamos a escalar la red hasta los 255 equipos y no necesitamos más.

IPv6 estará deshabilitado por seguridad.

### Direccionamiento IP y subredes

Consultar el ANEXO 1 y 2

## Administración de servidores

### Sistemas operativos y software

Servidores: VMware vSphere Hypervisor (ESXi), VMware vCenter Server, Windows Server 2022 standard, donde habrá máquinas virtuales en función de los proyectos.

Trabajadores: Todos los ordenadores de los trabajadores llevan Windows 10 pro.

Software Servidores: Instalaremos Pulseway para la administración remota de Windows Server, un antivirus, software de copias de seguridad.

Software Trabajadores: Utilizaremos cuentas corporativas de Google para usar sus servicios, visual studio para los programadores y desarrolladores, antivirus, software de copias de seguridad.

### Servicios en red

Los servicios presentes son los siguientes: DNS, DHCP, SMB para los trabajadores que tengan que almacenar sus datos de trabajo, además de las copias de seguridad, una VPN y RDP por si los trabajadores tienen que trabajar desde casa, Active Directory para la gestión de los usuarios, para las actualizaciones de Windows WSUS y para la autentificación de los empleados en las redes corporativas RADIUS.

### Active Directory - Usuarios y Grupos

Cada departamento tendrá su grupo y su unidad organizativa con un nombre identificativo del departamento, además los usuarios se identificarán con nombre y apellidos y se meterán dentro de los grupos de trabajo correspondientes para la gestión de los permisos.

### Active Directory – Recursos compartidos y cuotas de disco

El servidor de Active Directory tendrá recursos compartidos del NAS con los departamentos de programadores y desarrolladores para guardar sus proyectos en carpetas compartidas con la siguiente nomenclatura: Nombre departamento->Proyecto->Nombre del trabajador.

Los permisos de cada usuario solo afectan a su carpeta, no pueden ver el trabajo del resto de sus compañeros a no ser que sea necesario, para garantizar la seguridad.

Además, los usuarios solo pueden escribir 50 GB en disco, sin posibilidad de superar dicha cantidad, a no ser que se le amplié por alguna circunstancia.

### Sistemas de seguridad

Para evitar los inicios de sesión no autorizado contaremos con una autentificación en 2 factores.

Los usuarios deberán cambiar la contraseña cada 2 meses

Se activarán las horas activas para que no se pueda iniciar sesión cuando estas fuera del horario establecido.

Los discos duros de los ordenadores de trabajo estarán cifrados.

Los trabajadores no pueden modificar ningún parámetro de los sistemas de seguridad tales como antivirus, firewall.

Se van a grabar las acciones de un usuario o un grupo en el registro de eventos.

### Directivas de grupo

Se configurar las actualizaciones gradualmente, es decir, primero habrá un ordenador de cada departamento que reciban las actualizaciones antes que los demás, para verificar que todo sigue funcionando y no hay ningún error. Si no hay ningún error, el resto de los ordenadores se actualizarán en el tiempo establecido por el administrador de red. Y si falla en los primeros ordenadores se pausará la actualización en el resto para que el fallo no se extienda.

Más información de esta política [Windows Update for Business](https://docs.microsoft.com/es-es/windows/deployment/update/waas-wufb-group-policy).

Implementar Windows hello para el inicio de sesión. [Directivas de Windows Hello](https://docs.microsoft.com/es-es/windows/security/identity-protection/hello-for-business/hello-key-trust-policy-settings).

Directiva para cifrar cualquier unidad extraíble. [Directivas de grupo de BitLocker](https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings)

Directiva para activar la protección del DMA del kernel.

El fondo de pantalla se les cambiará en función del departamento.

## Administración de clientes

### Acceso clientes

Los clientes tendrán acceso a un portal cautivo, además de una aplicación para dispositivos móviles donde podrán gestionar los dispositivos que adquieran, con el añadido de que todos los productos son compatibles con el asistente de Google, Alexa, etc…, por lo que también se pueden controlar por voz.

Los clientes deberán crearse una cuenta de Bionica Automations para poder acceder a la app y el portal cautivo, está se asociará con la cuenta Google, Amazon, otros, para el control por voz.

### Sistemas de seguridad

Los clientes pueden activar si lo desean una verificación en 2 factores para añadir más seguridad a la cuenta.

Todas las comunicaciones están cifradas con protocolos seguros de comunicación.

## Ciberseguridad

### Inventario de Activos

#### Resumen

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 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: [Pricing](https://www.pulseway.com/pricing)

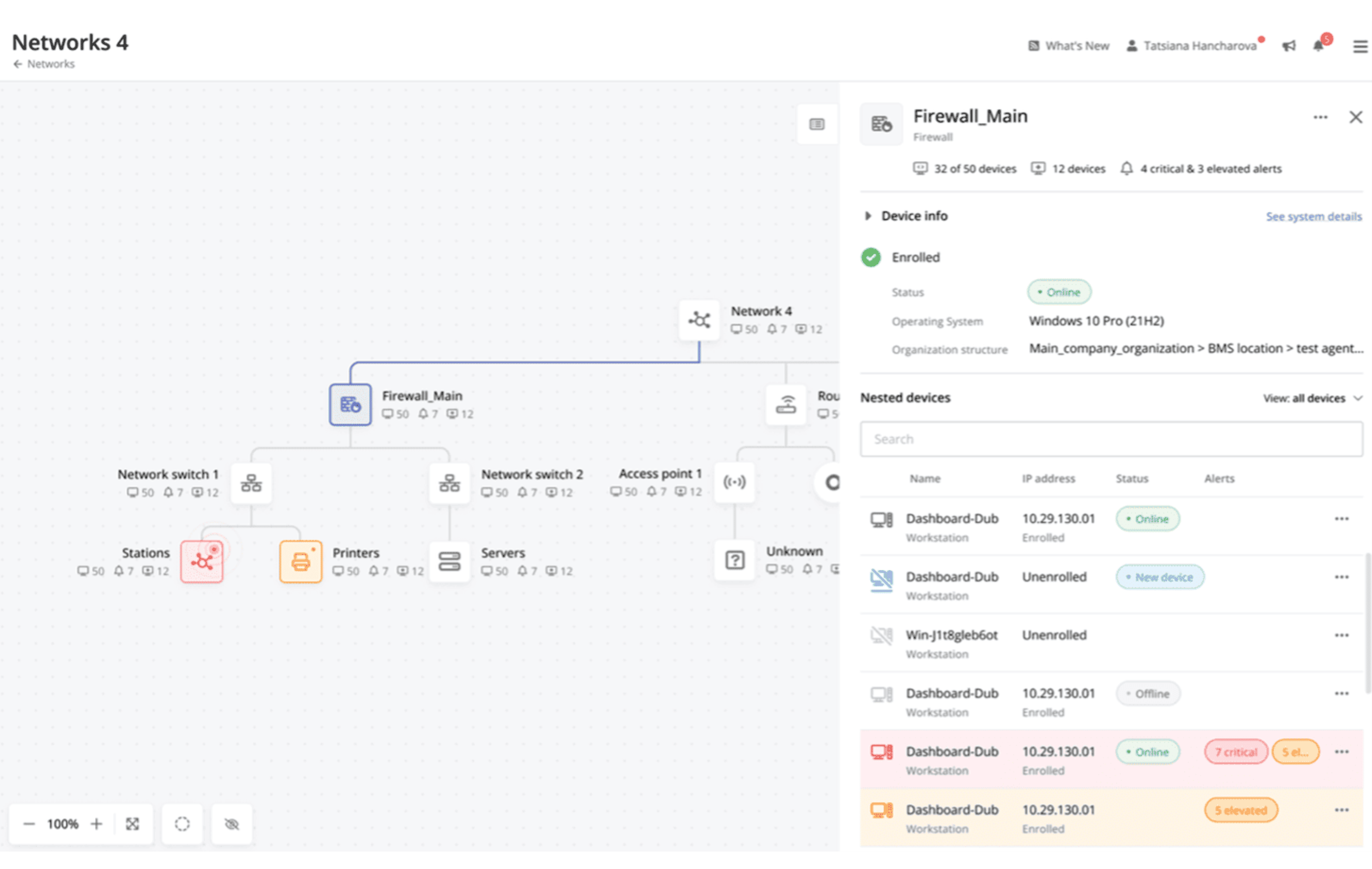
Las características de este software son las siguientes:

* [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)

#### Administración de dispositivos

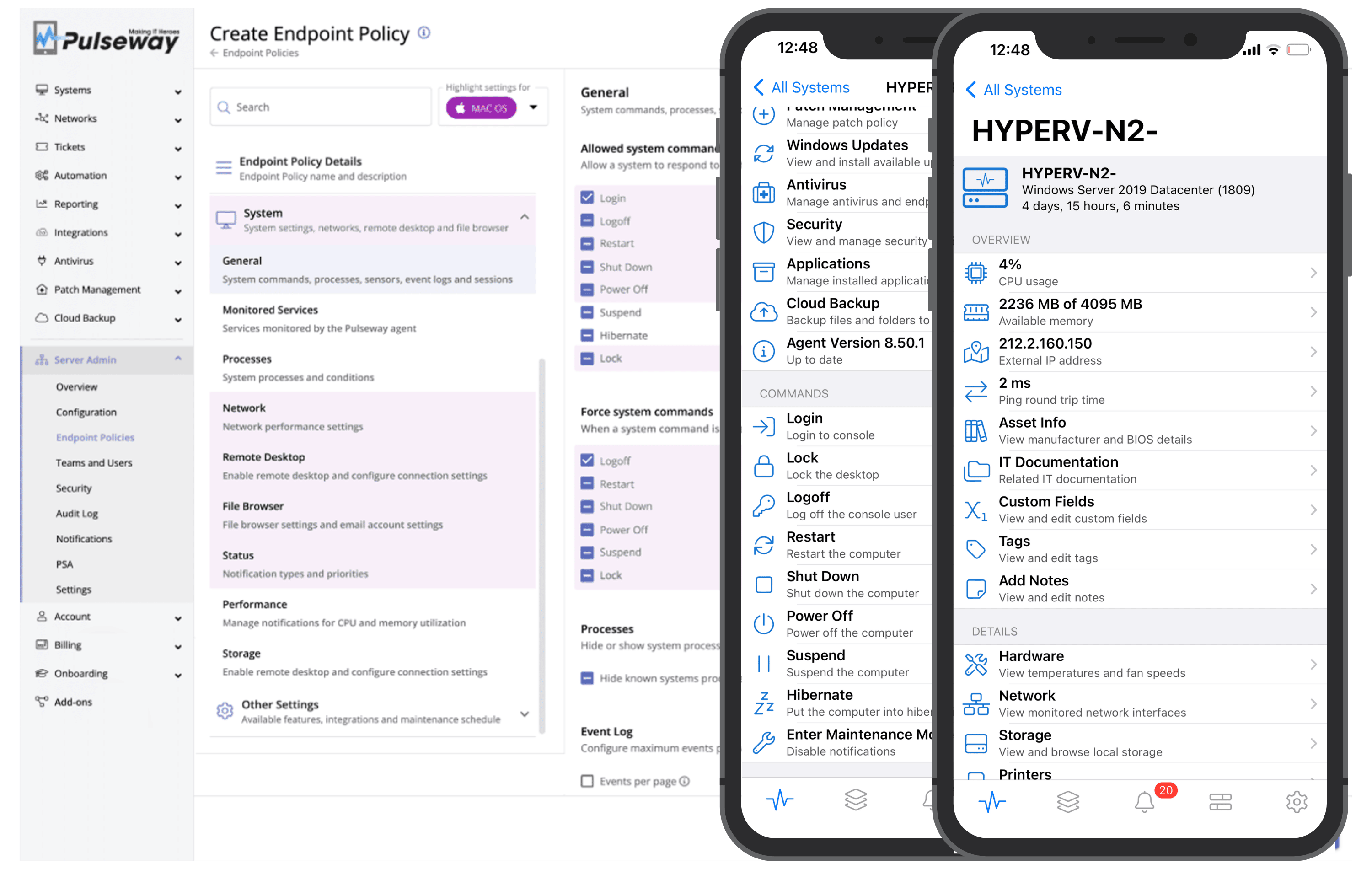
Dentro de este apartado se engloba todas las funcionalidades que tienen que ver con la administración IT de activos:

##### Descubrimiento y despliegue



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.

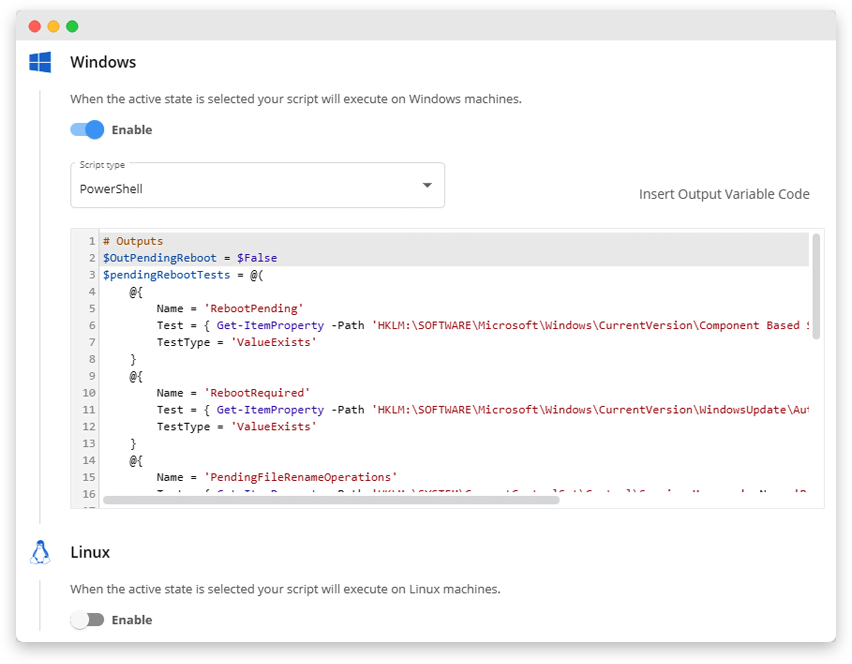
##### Monitorización y administración



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.

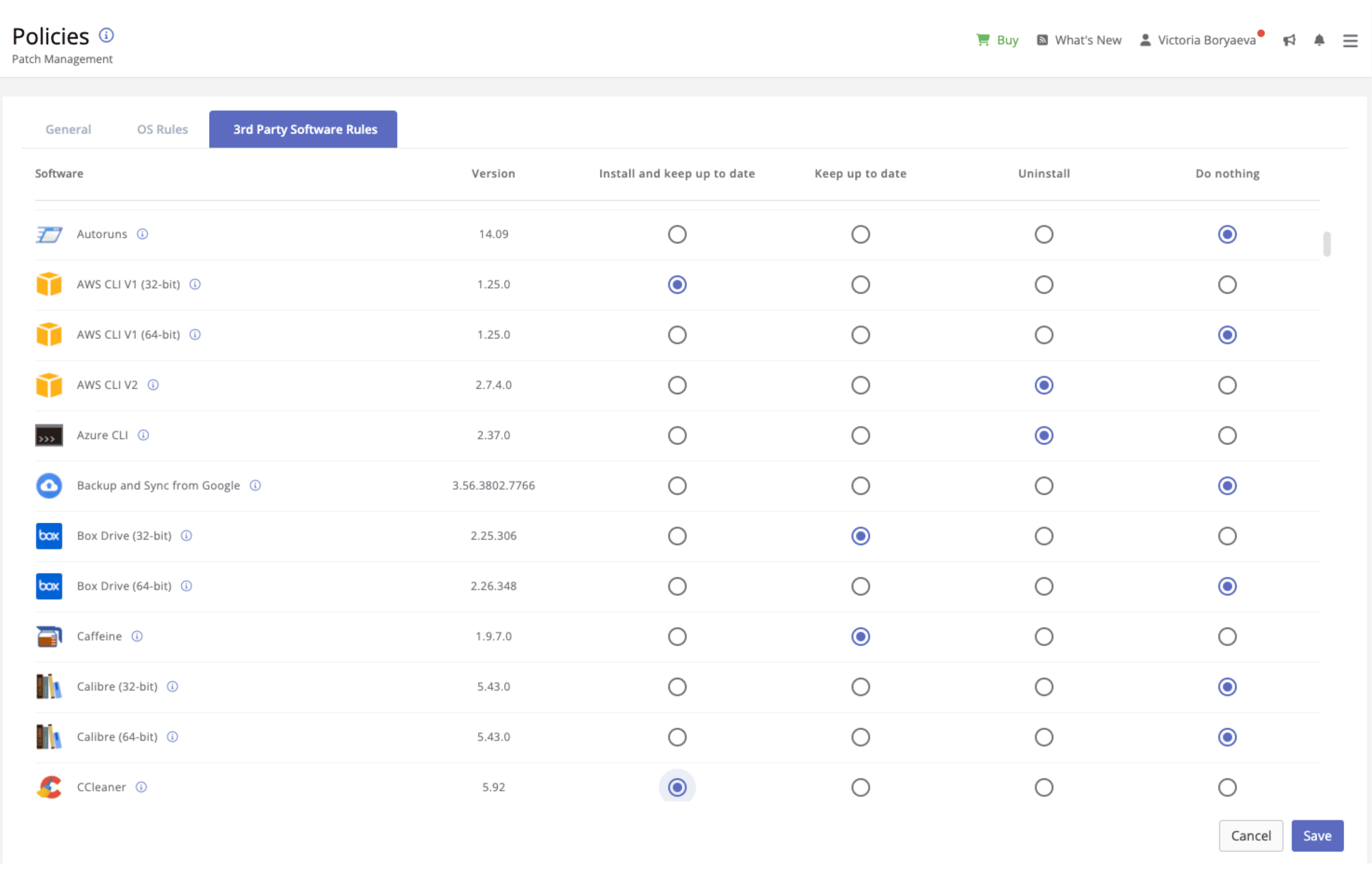
Desea ofrecer el mismo nivel de servicio a todos sus clientes y con la aplicación de administración de TI móvil más rica en funciones de la industria, puede hacerlo. Su equipo ahora puede hacer su trabajo desde cualquier lugar para que puedan responder rápidamente a cualquier problema, de cualquier cliente,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

##### Automatización y auto remediación



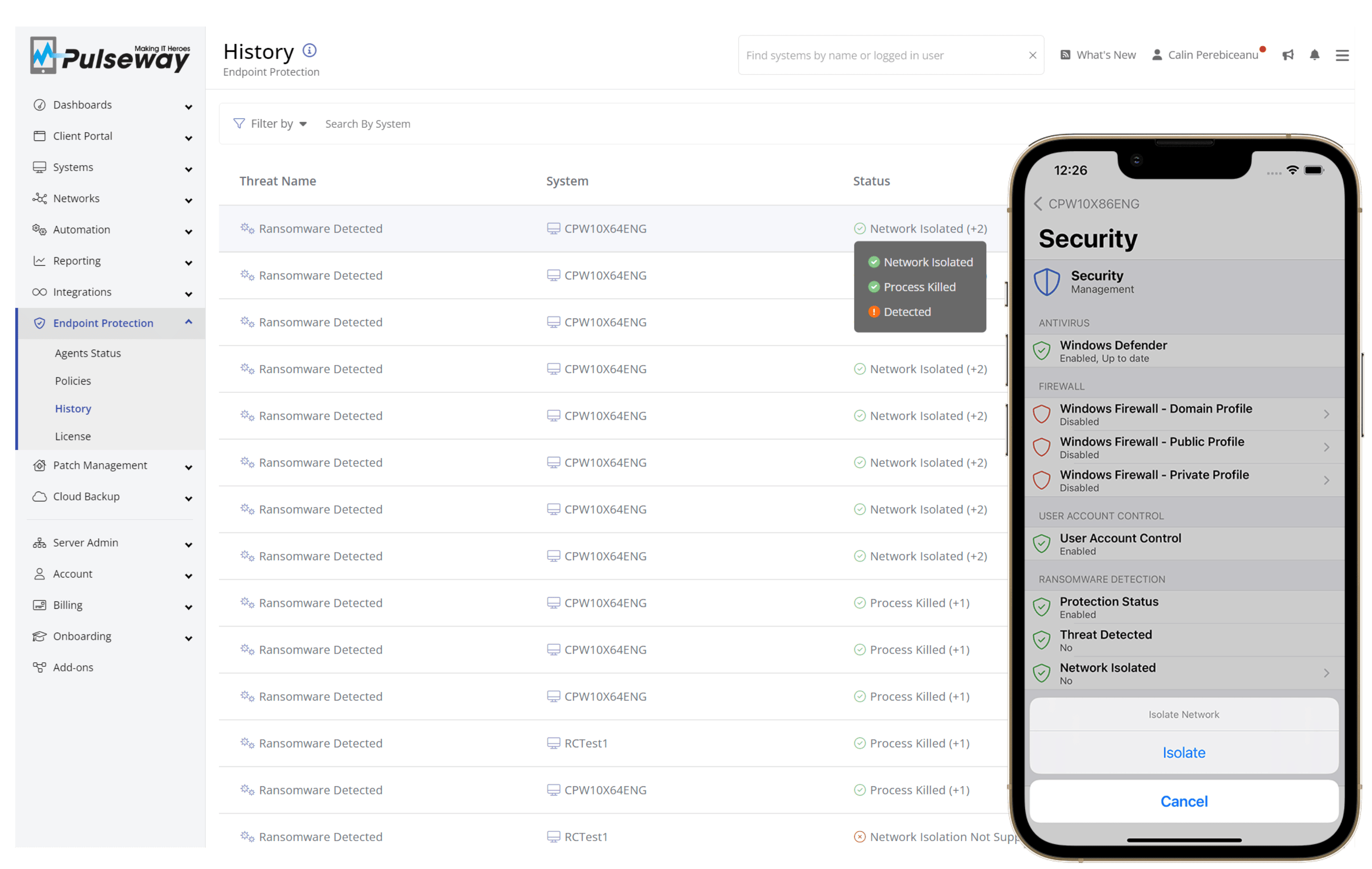
Haga más haciendo menos, con el potente motor de automatización de Pulseway. Al combinar la tecnología de flujo de trabajo con una interfaz de usuario intuitiva, puede configurar activadores inteligentes para solucionar automáticamente los problemas de TI de inmediato antes de que tengan la oportunidad 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.

##### Administración de 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.

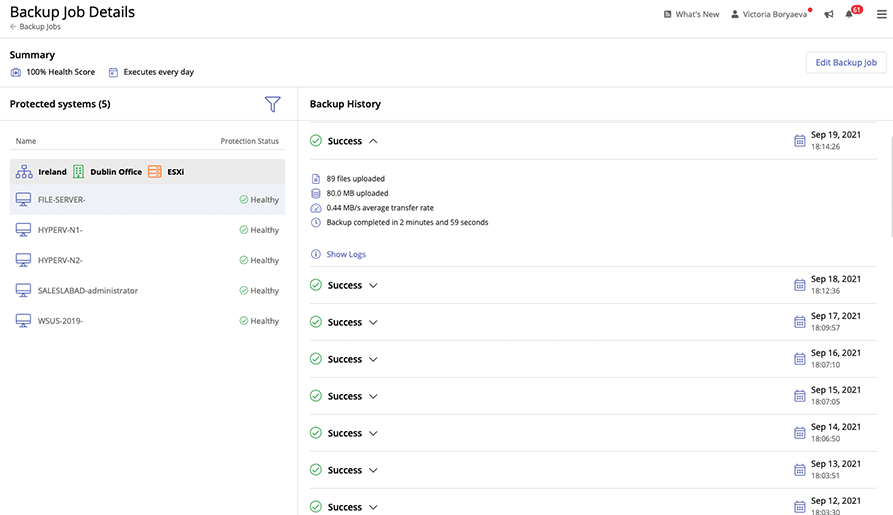
##### Detección de Ransomware y AV integrado



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.

#### 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.



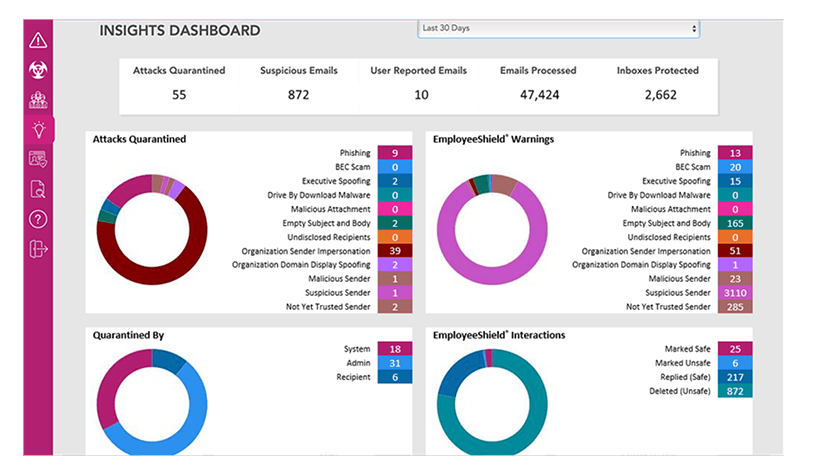
Muchos usuarios de estas plataformas no se dan cuenta de que no están protegidos contra la pérdida de datos causada por una acción accidental o maliciosa del usuario, y necesitan hacer sus propios arreglos de copia de seguridad.

#### 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.

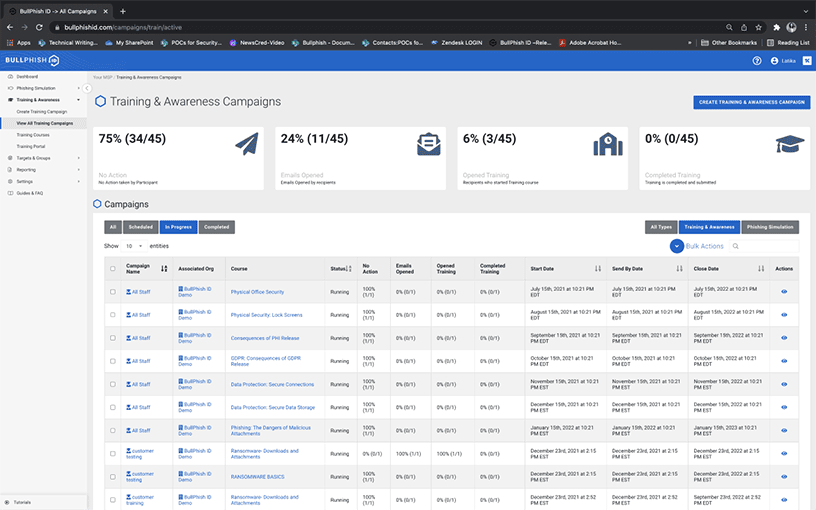
##### Protección contra Phishing



**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.

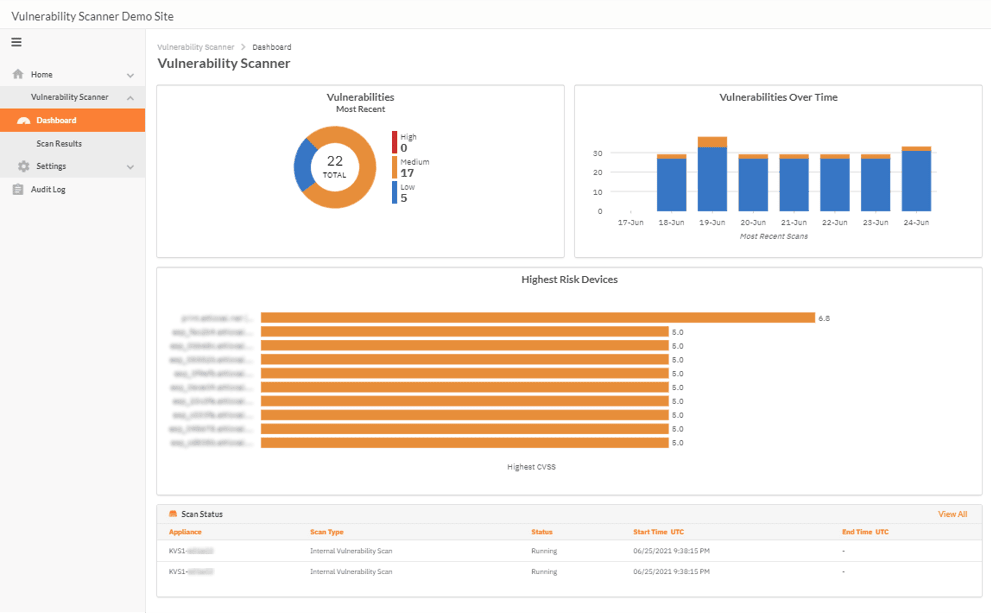
##### Planes de concienciación



**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.

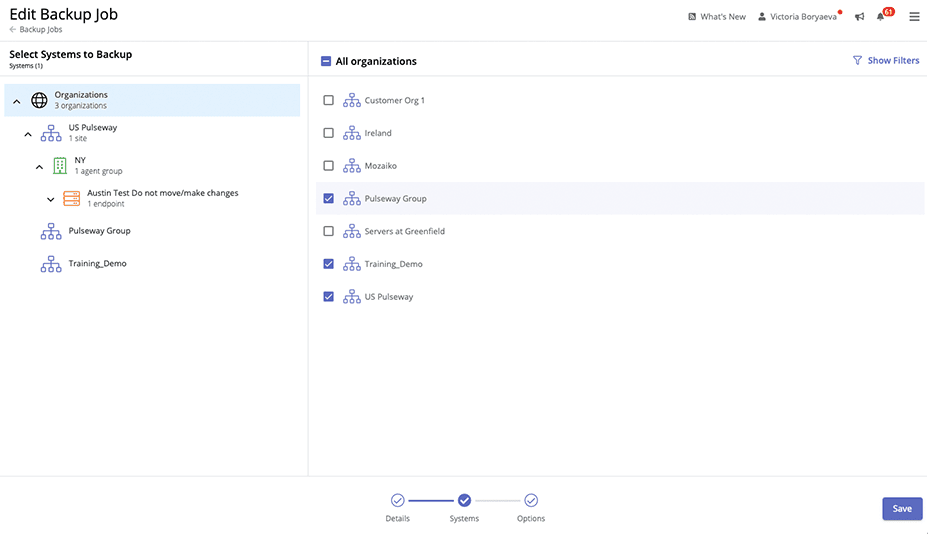
* Agregue a todos los empleados a su equipo de seguridad con capacitación en concientización sobre seguridad que les permite detectar y detener las amenazas de phishing.
* Automatice las campañas de capacitación y los informes para obtener una capacitación consistente y sin estrés que obtenga resultados.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

##### 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.

##### Backup and 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.

### Firewall

#### Firewalls de red (Router)

Las conexiones de fuera hacia dentro están bloqueadas y las conexiones salientes permitidas.

Si permitimos que los trabajadores trabajen desde casa se dispondrá de una VPN a los recursos de la empresa.

#### Firewalls de los ordenadores

Por defecto con el perfil de red corporativa.

#### Firewalls de los servidores

Expuestos solo los servicios necesarios.

### Switches

Los switches tendrán un faltado por Mac que va por puerto, si conectas un ordenador con distinta Mac que el que había antes, el puerto de deshabilitará.

### Antivirus

#### Para todos los equipos

Vamos a usar el antivirus de Panda con los servicios de Panda Systems Management, Panda Fusion, Panda Fusion 360, Panda Email Protection, Panda Patch Management, Panda Full Encryption, Aether Platform.

### Directivas de seguridad

Más información de esta política [Windows Update for Business](https://docs.microsoft.com/es-es/windows/deployment/update/waas-wufb-group-policy).

Implementar Windows hello para el inicio de sesión. [Directivas de Windows Hello](https://docs.microsoft.com/es-es/windows/security/identity-protection/hello-for-business/hello-key-trust-policy-settings).

Directiva para cifrar cualquier unidad extraíble. [Directivas de grupo de BitLocker](https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings)

Directiva para activar la protección del DMA del kernel.

Poner el número mínimo de caracteres para las contraseñas.

Las contraseñas no se pueden repetir y tienen que cumplir una serie de criterios.

Las contraseñas se cambiarán cada 2 meses.

### Copias de seguridad

El software de copias de seguridad que vamos a utilizar es Easeus la edición Advanced Server.

#### Análisis

Los datos más importantes que podemos tener son los siguientes:

* Sistema operativo de Windows Server de Active Directory (aunque sea una VM, la copia se hará aparte).
* El resto de los servicios que están en otras máquinas virtuales asociadas a los proyectos.

La información de los proyectos puede cambiar seriamente cada hora, los datos de contabilidad cada día, los datos de los clientes cada media hora, el sistema operativo de Windows server de Active Directory cada 1 semanas, el resto de las máquinas virtuales cada 1 semanas también.

Los datos de los proyectos se almacenarán durante 6 meses, los de contabilidad durante 3 años, los datos de los clientes durante 1 año, el S.O. del Windows Server de Active Diectory se almacenará durante 4 meses, el resto de los servicios de otras máquinas virtuales de proyectos se almacenarán durante otros 6 meses.

#### Diseño

En el siguiente esquema relacionado con el horario en el que se van a ejecutar las copias de seguridad y su ubicación, no están incluidas las copias de los datos de los clientes (Base de datos de clientes), ya que esto hay que hablarlo con la empresa que contratemos para dichos servicios para acordar un plan de copias de seguridad.

### Puesto de trabajo

Consultar el Anexo 3 documento:

UBALDE\_Plan\_de\_Ciberseguridad\_en\_puestos\_de\_trabajo

Anexo 1 - Diagrama Packet tracer

[Anexos\Anexo 1 - Diagrama Packet Tracer](Anexos/Anexo%201%20-%20Diagrama%20Packet%20Tracer)

Anexo 2 - Esquema de conexiones

Se detallan todas las conexiones cableadas de los ordenadores y dispositivos de la empresa.

[Anexos\Anexo 2 - Esquema de conexiones](Anexos/Anexo%202%20-%20Esquema%20de%20conexiones)

Anexo 3 – Plan de ciberseguridad

[Anexos\Anexo 3 - Ciberseguridad](Anexos/Anexo%203%20-%20Ciberseguridad)

Anexo 3 – Plan de ciberseguridad

[Anexos\Anexo 4 - Plan copias de seguridad](Anexos/Anexo%204%20-%20Plan%20copias%20de%20seguridad/UBALDE_Plan_Copias_Seguridad.xlsx)