Informe técnico empresarial

HPE aruba networking

Conectividad de red impulsada por IA y centrada en la seguridad para el cumplimiento de NIS2

Acelerar el cumplimiento de NIS2 con HPE Aruba Networking

HPE GreenLake

Contenido

NIS2: Llevar un alto nivel común de ciberseguridad a la UE

La Directiva sobre seguridad de redes y sistemas de información (NIS2) es una normativa histórica y exhaustiva de la Unión Europea (UE) en materia de ciberseguridad, concebida para impulsar el nivel general de ciberseguridad en la UE[1]. Basada en la Directiva NIS de 2018, la primera disposición legislativa de la UE sobre ciberseguridad[2], la NIS2 se adoptó en diciembre de 2022 como respuesta a la creciente digitalización y al aumento de las amenazas a la ciberseguridad derivadas de la pandemia COVID-19 y del conflicto entre Rusia y Ucrania. Las reglamentaciones de NIS2 amplían el alcance de las organizaciones sujetas a los requisitos de ciberseguridad de la UE.

Se espera que más de 100 000 organizaciones se vean afectadas por las normas de ciberseguridad de NIS2 que los Estados miembros de la UE deben implementar a partir del 17 de octubre de 2024[3].

Cualquier organización (1) con más de 250 empleados o 50 millones de euros de ingresos anuales que preste sus servicios dentro de la UE (2) y en un sector catalogado como «entidades esenciales e importantes» debe cumplir las directivas NIS2[4]. Entre los sectores sujetos ahora al cumplimiento del NIS2 figuran la administración pública y los gobiernos locales; la producción, transformación y distribución de alimentos; los servicios postales y de mensajería; y la industria manufacturera y los proveedores digitales.[5]. Las organizaciones de los sectores sujetos a anteriores requisitos de la Directiva NIS también deben cumplir los mandatos de la NIS2; entre estos sectores se incluyen la sanidad, la banca y las finanzas, y el transporte. (Nota: Esta lista no es exhaustiva. Para más información, consulte los anexos 1 y 2 de la Directiva NIS2[6].)

Desafíos de cumplimiento de NIS2

Tanto si se trata de implementar tecnología y prácticas conformes por primera vez como de añadir capacidades para satisfacer requisitos más amplios, el cumplimiento de la normativa puede suponer a menudo un reto para las organizaciones.

Requisitos entre dominios: los marcos de cumplimiento como NIS2 suelen abarcar dominios tecnológicos dentro de una organización, lo que repercute en las prácticas y la infraestructura del extremo a la nube.

Capacidades fragmentadas: las capacidades necesarias para cumplir con NIS2 a menudo abarcan múltiples soluciones tecnológicas, lo que puede conducir a la adopción poco sistemática de productos puntuales. Con el tiempo, este enfoque de mosaico de la seguridad no solo aumenta la complejidad arquitectónica y operativa, sino que también expone a la organización a brechas de seguridad, incoherencias en las políticas y su aplicación, y posibles riesgos de ciberseguridad.

Colaboración en equipo: ofrecer una innovación exitosa que cumpla los requisitos de normativa a menudo requiere que los equipos de red y seguridad trabajen juntos para perseguir metas y objetivos comunes, proporcionando experiencias superiores a la vez que se mantiene a la organización a salvo de ataques cada vez más frecuentes y sofisticados.

Las multas por incumplimiento pueden alcanzar al menos 10 millones de euros o el 2 % de los ingresos totales anuales globales de las entidades esenciales[7].

[1] La directiva NIS2: Un alto nivel común de ciberseguridad en la UE. Parlamento Europeo. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[2] La directiva NIS2: Un alto nivel común de ciberseguridad en la UE. Parlamento Europeo. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[3] Sievers, T. Propuesta de directiva NIS 2.0: empresas cubiertas por el ámbito de aplicación ampliado y sus obligaciones. Int. Cybersecur. Law Rev. 2, 223–231 (2021). https://doi.org/10.1365/s43439-021-00033-8 (#Fn19)

[4] NIS2 se aplica a las organizaciones del anexo I y del anexo II no clasificadas como microempresas o pequeñas empresas. Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se deroga la Directiva (UE) 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. Definición de microempresa y pequeña empresa según la Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas. http://data.europa.eu/eli/reco/2003/361/oj

[5] Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se deroga la Directiva (UE) 2016/1148. Unión Europea.

[6] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) N.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2). http://data.europa.eu/eli/dir/2022/2555/oj. Diciembre de 2022.

[7] Directiva sobre medidas para un nivel elevado común de ciberseguridad en toda la Unión (Directiva NIS2) – Preguntas frecuentes. Comisión europea. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs. Junio de 2023.

Conectividad de red impulsada por IA y centrada en la seguridad para el cumplimiento de NIS2

Acelera tu viaje hacia el cumplimiento de NIS2 con conectividad de red impulsada por IA y centradas en la seguridad de HPE Aruba Networking. Creadas con los principios de confianza cero, las soluciones de red impulsadas por IA y centradas en la seguridad de HPE Aruba Networking proporcionan una base común para que los equipos de redes y seguridad impulsen experiencias distintivas y resultados de negocio innovadores sin sacrificar la protección de la ciberseguridad.

Una red impulsada por IA y centrada en la seguridad de HPE Aruba Networking facilita la adopción de la seguridad de confianza cero y respalda el cumplimiento de las normas y reglamentos de ciberseguridad al permitir que los equipos utilicen la red como solución de seguridad. Ahora, la red puede proporcionar visibilidad e información más avanzados, gestión de políticas centralizada, protección de datos, defensa frente a amenazas y control de acceso en una única plataforma. Con estas capacidades integradas de seguridad de confianza cero, la propia red se convierte en una línea de defensa crítica que ayuda a satisfacer los requisitos de NIS2 sin la complejidad añadida que suponen múltiples herramientas dispares, o el costoso y perturbador requisito de desinstalación y sustitución de la infraestructura existente.

La conectividad de red impulsada por IA también multiplica el poder humano de una organización, un factor crucial a medida que se amplían los marcos normativos, se ensanchan las brechas de talento y aumentan las amenazas cibernéticas. Con la conectividad de red impulsada por IA y centrada en la seguridad de HPE Aruba Networking, los equipos pueden beneficiarse con la automatización automática que reduce el esfuerzo manual, mejora la visibilidad y la detección de anomalías, y mejora la supervisión y los diagnósticos, todo lo cual garantiza que la organización no se exponga a riesgos innecesarios.

Cumplir con los requisitos clave de NIS2 con HPE Aruba Networking

Las pautas de NIS2 abarcan una variedad de capacidades y requisitos que apuntan a reforzar la ciberseguridad regional y organizativa y la resiliencia empresarial. Las directrices incluyen requisitos para la detección y respuesta ante incidentes, estrategia y gobernanza de la ciberseguridad, y seguridad de infraestructuras y aplicaciones.

Prácticas de higiene cibernética básica

El preámbulo 89 de la Directiva NIS2 esboza una serie de requisitos de «higiene cibernética básica», prácticas fundamentales diseñadas para mejorar la postura de ciberseguridad y proteger a la organización de amenazas y vulnerabilidades[8].

Las soluciones de HPE Aruba Networking pueden ayudar a satisfacer los requisitos del preámbulo 89 para prácticas de higiene cibernética básica, entre las que se incluyen las siguientes:

- Principios de seguridad de confianza cero
- Gestión de identidad y acceso o conocimiento del usuario
- Segmentación de red
- Integración de tecnologías de mejora de la ciberseguridad, como inteligencia artificial o aprendizaje automático
- Actualizaciones de software
- Configuración de dispositivos

Seguridad de confianza cero

Aunque ningún proveedor o solución puede ofrecer por sí solo toda la protección cibernética que necesita una organización, comenzar con una red que proporcione una base integrada para la seguridad de confianza cero puede ayudar a reducir el número de herramientas dispares necesarias para cumplir los requisitos de NIS2, al tiempo que añade protección en los puntos de entrada digitales críticos.

HPE Aruba Networking Edge Services Platform (ESP) se basa en los principios de seguridad de confianza cero del extremo a la nube, lo que mejora la protección al tiempo que simplifica las operaciones. HPE Aruba Networking ofrece capacidades de confianza cero —con visibilidad integral, autenticación y autorización, y controles de acceso con privilegios mínimos, así como supervisión continua y aplicación de políticas— en sintonía con el ecosistema de seguridad más amplio, dentro y fuera de la red corporativa.

[8] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) N.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2). Unión Europea.

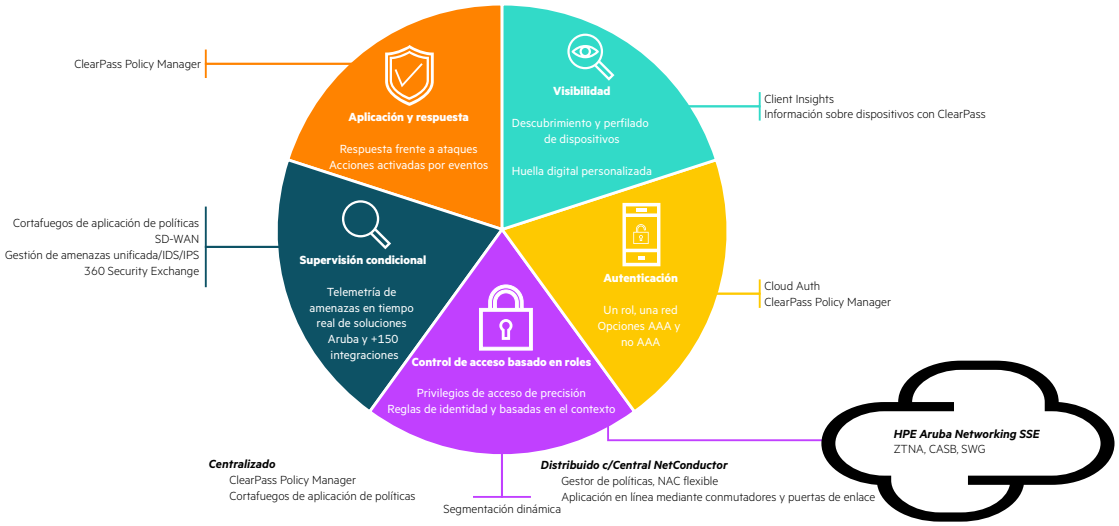

Figura 1. Fundamentos de la seguridad de confianza cero con HPE Aruba Networking

Gestión de identidades y accesos

La seguridad de confianza cero comienza con la visibilidad de los usuarios conectados y sus dispositivos. La solución de gestión de red basada en la nube **HPE Aruba Networking Central** incluye visibilidad y creación de perfiles impulsados por IA con **Client Insights**. Client Insights analiza la telemetría nativa de la infraestructura directamente desde puntos de acceso, conmutadores, puertas de enlace y clientes, sin necesidad de instalar colectores o agentes físicos. Client Insights proporciona perfiles precisos de dispositivos con inteligencia artificial/aprendizaje automático con hasta un 99 % de precisión en clientes conocidos con una tasa <5 % de desconocidos a través de una amplia variedad de puntos finales que se conectan a la red, entre ellos un conjunto diverso de dispositivos IoT en toda la infraestructura cableada e inalámbrica[9]. Para los entornos no gestionados de forma externa por HPE Aruba Networking Central basado en la nube o con dispositivos de red de terceros, **HPE Aruba Networking ClearPass Device Insight** proporciona identificación y creación de perfiles de clientes basada en aprendizaje automático.

Gana hasta un 99 % de precisión en la elaboración de perfiles para dispositivos conectados a la red, incluidos los de IoT

Una vez conocido y perfilado un usuario o dispositivo, el siguiente paso es autentificar su identidad cada vez que se conecte a la red. Con **HPE Aruba Networking ClearPass**, autentica usuarios y dispositivos a partir de una amplia variedad de fuentes de identidad, como Active Directory. Mediante un rico motor de políticas que permite privilegios de acceso precisos, ClearPass controla qué usuarios y qué dispositivos pueden acceder a qué recursos. Las políticas siguen al usuario y al dispositivo sin fisuras a través de redes cableadas, inalámbricas y de área extensa, incluso en entornos de varios proveedores.

Para las redes gestionadas por HPE Aruba Networking Central, la solución el control de acceso a la red (NAC) nativo de la nube **Cloud Auth** permite la incorporación sin fricciones de usuarios finales y dispositivos cliente, ya sea mediante autenticación basada en la dirección MAC o mediante integraciones con almacenes de identidad en la nube comunes, como Google Workspace™ o Azure Active Directory para asignar automáticamente el nivel adecuado de acceso a la red.

Para los usuarios híbridos y remotos, así como para terceros como contratistas y trabajadores temporales, **el acceso a la red de confianza cero (ZTNA) HPE Aruba Networking SSE** limita el acceso, a través de un agente de confianza, solo a aplicaciones específicas o microsegmentos que han sido aprobados para el usuario, tal como se define a través de una única interfaz de política global. La monitorización continua garantiza que las políticas se adapten automáticamente basándose en cambios de identidad, ubicación y estado del dispositivo, lo que hace más fácil asegurar la confianza cero en cada actividad de acceso.

[9] Aruba ayuda a los equipos de red a superar la escasez de recursos de personal con la primera solución AIOps que combina información de red y seguridad para mejorar la eficiencia de TI. https://www.businesswire.com/news/home/20220726005426/en/Aruba-Helps-Network-Teams-Overcome-Scarce-Staff-Resources-with-First-AIOps-Solution-that-Combines-Network-and-Security-Insights-for-Improved-IT-Efficiency; Infraestructura de red impulsada por IA: La respuesta para la eficiencia de la TI. https://www.arubanetworks.com/resource/ai-powered-network-infrastructure-the-answer-to-it-efficiency/

Segmentación de red

La segmentación dinámica de **HPE Aruba Networking** separa el tráfico de la red en función de la identidad y los permisos de acceso asociados, aplicando el acceso de confianza cero con privilegios mínimos a las aplicaciones y los datos del extremo a la nube. La segmentación dinámica admite múltiples modelos de aplicación —centralizada y distribuida—, lo que permite al departamento de TI utilizar uno o ambos modelos en función de las necesidades del entorno. La aplicación centralizada la proporciona **Policy Enforcement Firewall**, un cortafuegos de aplicación completa integrado en la infraestructura de red de HPE Aruba Networking.

Para la aplicación distribuida en línea dentro de la infraestructura de puerta de enlace y conmutación, **HPE Aruba Networking Central NetConductor** utiliza tecnología ampliamente adoptada, como EVPN/VXLAN, para producir una superposición de red distribuida. Esta solución de pila completa incluye servicios de seguridad nativos de la nube para la gestión de políticas globales y la configuración de la red con una sencilla interfaz de lógica empresarial y flujos de trabajo intuitivos que los equipos de red y seguridad pueden utilizar para ofrecer un rendimiento óptimo de la red al tiempo que definen y aplican políticas de seguridad granulares que son la base de las arquitecturas de confianza cero.

Las organizaciones también pueden usar **HPE Aruba Networking EdgeConnect SD-WAN** para aplicar políticas de seguridad uniformes que abarquen la WAN y la LAN con capacidades globales de cortafuegos de próxima generación (NGFW) integradas, como IDS/IPS, protección ante ataques DDoS y microsegmentación en toda la empresa. Los servicios de NGFW integrados permiten a las organizaciones consolidar la red de sucursales y las funciones de seguridad eliminando los cortafuegos y enrutadores heredados en las sucursales.

Dentro del centro de datos, **HPE Aruba Networking Fabric Composer** facilita la implementación de la seguridad de confianza cero simplificando y automatizando el proceso de microsegmentación con una interfaz de usuario interactiva y fácil de usar. El **conmutador HPE Aruba Networking CX 10000** ofrece microsegmentación distribuida, cortafuegos este-oeste, cifrado y servicios de telemetría en línea, a través de cada puerto, más cerca de las aplicaciones empresariales críticas, eliminando la necesidad de cortafuegos adicionales.

La supervisión continua de los usuarios y dispositivos de la red es otra de las mejores prácticas de la Seguridad de confianza cero. Las soluciones HPE Aruba Networking se integran con más de 150 de las mejores soluciones de seguridad dentro de **Aruba 360 Security Exchange** para suministrar telemetría de amenazas en tiempo real procedente de múltiples fuentes y actuar en consecuencia. La comunicación bidireccional entre la red y el ecosistema de seguridad más amplio permite a las organizaciones aprovechar los datos de la red no solo para obtener visibilidad y control sobre la actividad de usuarios y dispositivos, sino también para aumentar el valor de sus inversiones.

Actualizaciones de software y configuraciones de dispositivos

HPE Aruba Networking Central simplifica el flujo de trabajo de configuración de los dispositivos gestionados al permitir a los administradores combinar un conjunto de dispositivos en grupos. Los grupos permiten a los administradores gestionar los dispositivos de forma eficaz mediante un flujo de trabajo de configuración basado en la interfaz de usuario o una plantilla de configuración basada en la CLI.

HPE Aruba Networking pone a disposición actualizaciones de rendimiento y seguridad del software a través de su galardonado **Portal de soporte**.

Premio 2023 TSIA STAR a la Innovación en Portales de Clientes que mejoran la experiencia digital del cliente

Gestión de riesgos

El artículo 21 de la Directiva NIS2 establece requisitos para las «medidas de gestión de riesgos de ciberseguridad», que abarcan medidas técnicas, operativas y organizativas tanto para gestionar los riesgos que se plantean para la seguridad de las redes y los sistemas de información como para prevenir o minimizar el impacto de los incidentes de seguridad.[10].

Las soluciones de HPE Aruba Networking cumplen los requisitos del artículo 21 relativos a las medidas de gestión de los riesgos de ciberseguridad, en particular.

- Desarrollo de software seguro
- Seguridad de la cadena de suministro
- Criptografía y cifrado
- Seguridad en la adquisición de redes y sistemas de información
- Uso de la autenticación continua
- Manejo de incidentes
- Continuidad del negocio
- Notificación y resolución de vulnerabilidades

Desarrollo de software seguro

Descubre cómo HPE Aruba Networking emplea procesos de desarrollo seguro para reducir las vulnerabilidades a la vez que optimiza los costos y la disponibilidad de las soluciones. Desarrollar productos de acuerdo con las mejores prácticas del **ciclo de vida de desarrollo de software y del marco de desarrollo seguro de software** ayuda a proteger a las organizaciones de una exposición innecesaria al riesgo.

- **Análisis de requisitos:** analizar los riesgos de seguridad y establecer requisitos de seguridad de alto nivel.
- **Definición:** realizar modelos y análisis de amenazas de seguridad.
- **Diseño:** diseñar para mitigar los riesgos de seguridad según los requisitos. Identificar los componentes de código abierto y de terceros.
- **Codificación:** reutilizar los componentes protegidos. Implementar prácticas de codificación seguras. Revisar el código y usar herramientas de análisis estático del código.
- **Pruebas:** probar las características de seguridad realizando análisis de seguridad, validación de entradas y pruebas de penetración para lograr una configuración segura.
- **Implementación:** firmar digitalmente el software (firma de código) para verificar la integridad del código. Analizar para detectar malware y hacer una revisión del código abierto. Entregar la lista de materiales de software (SBOM).
- **Mantenimiento:** publicar en el portal de soporte de HPE Aruba Networking. Reparar y mantener las versiones según sea necesario.

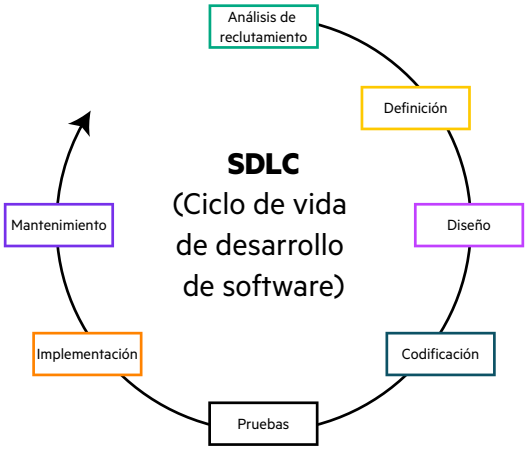

Figura 2. Ciclo de vida de desarrollo de software (SDLC)

[10] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) N.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2). Unión Europea.

Seguridad de la cadena de suministro

HPE es líder en el sector de las TIC para la ciberseguridad de la cadena de suministro. Las soluciones de HPE Aruba Networking se construyen utilizando únicamente SKU certificadas **conformes con la TAA**, lo que reduce la probabilidad de que los componentes de hardware y software del producto hayan sido manipulados por alguien en un país hostil.

(Para cumplir los requisitos de la TAA, los productos deben fabricarse o «transformarse sustancialmente» en Estados Unidos o en un «país designado» por la TAA.[11])

Las soluciones se entregan con **una lista de materiales de software** para la gestión de riesgos de los componentes de software. A medida que evolucionan las amenazas de ciberseguridad, HPE Aruba Networking continúa identificando y mitigando los riesgos de ciberseguridad dentro de nuestra cadena de suministro y proporcionando productos seguros para que las organizaciones puedan concentrarse en sus objetivos empresariales.

Construir sobre una base segura

Las soluciones de HPE Aruba Networking han sido certificadas y/o validadas con rigurosas normas del Gobierno de EE.UU., lo que demuestra una **criptografía comprobada** y resistencia a los ataques. Las soluciones HPE Aruba Networking han sido evaluadas y autorizadas para su uso de conformidad con los mandatos y programas de ciberseguridad de EE.UU., como Common Criteria, FIPS-140, DoDIN-APL y USGv6, lo que demuestra que las soluciones cumplen los estrictos requisitos de seguridad.

La infraestructura HPE Aruba Networking fue seleccionada para redes clasificadas y no clasificadas dentro del Pentágono, sede del Departamento de Defensa de los Estados Unidos, dando soporte a más de decenas de miles de dispositivos diariamente. El Pentágono también amplió su despliegue de ClearPass Policy Manager para el control de acceso seguro a sus redes[12].

Para protegerse contra el código de arranque malicioso y los ataques de suplantación de dispositivos, las soluciones de redes inalámbricas y por cable HPE Aruba Networking utilizan la **tecnología de módulo de plataforma segura (TPM),** un estándar internacional para un criptoprocesador seguro y resistente a las manipulaciones diseñado para proteger el hardware mediante la integración de claves criptográficas en los dispositivos. Instalada durante la fabricación, la tecnología TPM puede proporcionar una raíz de confianza segura sobre la que construir capas adicionales de seguridad de confianza cero y extremo de servicio de acceso seguro (SASE).

Para evitar que los puntos de acceso no autorizados obtengan acceso de puerta trasera a la red e intercepten los datos de los usuarios, HPE Aruba Networking Central ofrece prevención avanzada de **intrusiones inalámbricas**. Los equipos de redes y seguridad pueden establecer reglas personalizadas para la detección de puntos de acceso no autorizados en función de sus propios umbrales de riesgo.

Notificación y resolución de vulnerabilidades

HPE Aruba Networking Threat Labs gestiona y mitiga las vulnerabilidades de seguridad en los productos HPE Aruba Networking. Las vulnerabilidades pueden ser notificadas por investigadores de seguridad independientes, clientes o incluso empleados de HPE Aruba Networking. HPE Aruba Networking también gestiona un programa público de recompensas por errores, que puede descubrir vulnerabilidades más rápidamente.

[11] Reglamento Federal de Adquisiciones: 52.225-5 Acuerdos comerciales. Gobierno de los Estados Unidos. https://www.acquisition.gov/far/52.225-5.

[12] El Pentágono moderniza la conectividad cableada e inalámbrica, en todos los niveles de clasificación, con la infraestructura de Aruba. https://www.businesswire.com/news/home/20201026005079/en/The-Pentagon-Modernizes-Wired-and-Wireless-Connectivity-Across-All-Classification-Levels-with-Aruba-Infrastructure. Octubre de 2020.

Continuidad del negocio

Las plataformas de red y gestión HPE Aruba Networking ofrecen una variedad de capacidades de resiliencia diseñadas para admitir operaciones mínimamente ininterrumpidas y un tiempo de actividad de red mejorado, incluidas la conmutación por error sin impacto, las actualizaciones de software en servicio, las actualizaciones de software mejoradas VSF, las actualizaciones en vivo y el diseño de alta disponibilidad.

Complementa las soluciones HPE Aruba Networking con recuperación ante desastres y copia de seguridad como servicio HPE GreenLake, que utiliza copias de seguridad cifradas para proteger las cargas de trabajo locales y nativas de la nube frente a ataques de ransomware, y HPE Services, que puede ayudarte a establecer políticas de seguridad de sistemas de información y gestión de riesgos adaptadas a tu organización.

Conclusión

Sin un enfoque estratégico de la simplificación y la colaboración, puede resultar difícil aplicar los mandatos exhaustivos de cumplimiento de NIS2. Con la conectividad de red impulsada por IA y centrada en la seguridad de HPE Aruba Networking, la red puede convertirse en un activo para tu organización que ayude a los equipos a alcanzar objetivos compartidos de seguridad, privacidad y cumplimiento.

Para obtener más información, visita https://www.arubanetworks.com/es/products/security/

Recursos adicionales

Innovación en la seguridad de la cadena de suministro de HPE: Aumentar la confianza y la resistencia del extremo a la nube

Política de respuesta a incidentes de seguridad de productos | HPE Aruba Networking

Formación y certificación en ciberseguridad | HPE Services - Educación

Toma la decisión de compra correcta. Contacta con nuestros especialistas en preventa.

Contáctanos

Visita **ArubaNetworks.com**

BWP_NIS2Compliance_RVK_020224 a00137587ese

Hewlett Packard Enterprise