Estrategias de ciberseguridad en empresas proveedoras de equipo y tecnología:

El caso de Huawei

Eduardo Ulises Galicia Galicia
José Luis Solleiro Rebolledo

Introducción

Huawei es una compañía perteneciente al sector de la electrónica y las telecomunicaciones, el cual que se encuentra en constante cambio debido a que presenta una alta tasa de innovación y un reemplazo rápido de tecnología. En este sentido, la compañía se caracteriza por una serie de estrategias corporativas que le permiten: a) conciliar los intereses individuales de sus trabajadores y sus objetivos personales con los objetivos de desarrollo de largo plazo de la compañía; b) sostener y desarrollar una fuerte cultura de innovación abierta; y c) consolidar una expansión en el extranjero a partir de un modelo de negocio inclusivo. Todo lo anterior le ha permitido a la compañía mantenerse a la vanguardia en el mercado mundial.

La estrategia de innovación en Huawei se basa en tres pilares fundamentales: investigación y desarrollo para mejorar y expandir sus productos y servicios, incluyendo la creación de soluciones innovadoras y la adquisición de tecnologías emergentes; colaboración con universidades y empresas para aprovechar recursos innovadores y compartir conocimientos; y apoyo a proyectos de universidades e institutos de investigación para desarrollo de tecnologías y de talento (Huawei Technologies, s.f.a).

La inversión de Huawei en investigación y desarrollo (I+D) a nivel global es destacada y ha aumentado significativamente en los últimos años. En 2022, la inversión en investigación y desarrollo creció hasta el 25% de la facturación global de la empresa, lo que supone una mejora significativa en comparación con el pasado (Verjan, 2023). Además, Huawei es la segunda empresa privada del mundo que más invierte en investigación y desarrollo (I+D), con inversiones de alrededor de 21 000 millones de dólares en 2020, lo que representa el 15.9% de sus ingresos globales. Este compromiso con la innovación y el desarrollo tecnológico le ha permitido a Huawei mantenerse como líder en la industria de las TIC y conservar una posición elevada en el *ranking* de las empresas que más invierten en I+D.

Por otro lado, actualmente se reconoce globalmente que el desarrollo de las tecnologías digitales (Inteligencia Artificial, Internet de las Cosas o Computación en la Nube) está asociado con nuevos retos y desafíos de seguridad, tales como la exfiltración de datos, el *malware*, el *ransomware*, los ataques distribuidos de denegación del servicio (DDoS) o el *phishing* (Solleiro *et al.*, 2022). Consciente de ello, Huawei ha adoptado una estrategia integral de ciberseguridad que tiene por objeto ofrecer productos confiables y de alta calidad al integrar, en todas las fases de sus procesos internos, líneas de acción que garanticen la protección y la seguridad de la información. A ello se añaden esfuerzos recientes para construir, al interior de la compañía, una comunidad de conocimiento sobre ciberseguridad y protección de la privacidad.

La ciberseguridad es, en consideración de Huawei, un tema prioritario y un desafío que requiere no sólo de un compromiso sólido por parte de la empresa, sino también de otros actores involucrados en el ecosistema de las tecnologías de la información y las comunicaciones (TIC), como los operadores de telecomunicaciones. En este sentido, la protección de la privacidad y de la confidencialidad de los datos personales confiere una responsabilidad compartida entre fabricantes, desarrolladores de aplicaciones y los operadores.

El presente documento tiene por objeto identificar los elementos centrales de la estrategia de ciberseguridad adoptada por Huawei. Para ello, la investigación se estructura de la siguiente manera: en la primera sección se aborda el marco corporativo de Huawei desde aquellas estrategias que le han permitido mantenerse a la vanguardia en el mercado mundial; en la segunda parte, posterior a un abordaje sintético sobre la definición y la relevancia de la ciberseguridad, se identifican tres de los elementos centrales de la estrategia de ciberseguridad de la compañía; en la tercera sección se describe el cumplimiento de las normas y, derivado de esto, las certificaciones más importantes con las que cuenta Huawei en la materia; en la cuarta sección se recupera el modelo de responsabilidad compartida en el que la compañía establece las responsabilidades que, en su consideración, corresponden a los actores del ecosistema TIC respecto a la protección de la privacidad y de los datos personales, y se destaca el papel específico que juegan los operadores de telecomunicaciones. Finalmente, en la sección de conclusiones se sintetizan los principales hallazgos de la investigación.

1. El marco corporativo de Huawei

Huawei es una compañía china establecida en 1987 en la ciudad de Shenzehn por Ren Zhengfei. De acuerdo con su sitio web (Huawei Technologies, 2022a), sus se orientan a tres tipos de clientes: **1)** Operadores de telecomunicaciones que proporcionan internet, banda ancha, servicios inalámbricos, y servicios de telefonía fija y celular; **2)** Empresas, instituciones y organizaciones diversas; y **3)** Consumidores finales que adquieren dispositivos inteligentes, como *smartphones*, relojes y computadoras portátiles.

De manera general, la compañía abarca cinco grandes áreas de negocio: **1)** Redes para empresas de comunicaciones públicas; **2)** Soluciones TIC para empresas, gobiernos, redes privadas, verticales de industria, generalmente a través de canales, distribuidores e integradores; **3)** Nube pública para empresas, consumidores y sector público (servidores, centros de datos, infraestructura de energía, etc.), en donde se identifica como la compañía Huawei Cloud, centrada en computación en la nube; **4)** Dispositivos para consumo final (*smartphones*, computadoras, *tablets*, etc.); y **5)** Generación de Energía Fotovoltaica para empresas, equipos de potencia y baterías para centros de datos y soluciones residenciales de energía fotovoltaica. La compañía se caracteriza por su cultura de innovación, en la que la tolerancia al fracaso (sin penalizaciones por el fracaso de ciertos proyectos de I+D), los incentivos a trabajadores, la orientación al cliente, y la autorreflexión[1] juegan un papel importante (Ding, 2018).

A lo largo de su trayectoria inventiva, el modelo de I+D de la compañía ha pasado de la operación aislada de sus departamentos, centrados meramente en la tecnología y la funcionalidad, a un desarrollo de productos impulsado por la demanda. De acuerdo con Wang *et al*. (2024), in 1999 (Wu, Murmann, Huang y Guo, 2020), Huawei adoptó el enfoque de *Integrated Product Development* (IPD)- desarrollo integral de producto- de IBM para reducir los costos asociados a y optimizar los procesos de I+D. Entre las estrategias asociadas a este enfoque destacan la estandarización de buenas prácticas, la digitalización de la información para hacerla de fácil acceso, la gestión de proyectos para mejorar la comunicación y la colaboración entre departamentos, y la gestión de requisitos para encontrar una hoja de ruta clara para el desarrollo de los productos a partir de la correcta comprensión de la demanda.

El éxito comercial y el rápido desarrollo de Huawei se fundamenta, de manera general, sobre tres grandes estrategias corporativas (figura 1). Desde el principio, la compañía ha destacado por su esquema de propiedad, pues a diferencia de otras multinacionales chinas, Huawei no pertenece al gobierno, sino a sus trabajadores gracias al Programa de Empleados

1 Mientras que los Red Teams son equipos encargados del diseño de productos, los Blue Teams son equipos de investigación que buscan errores y fallas en estos, las cuales, más tarde, serán defendidos y atendidos por los Red Teams. Este ambiente competitivo y de retroalimentación fomenta los procesos de innovación al interior de Huawei.

Accionistas adoptado desde su fundación (Huawei Technologies, 2022b). De acuerdo con Masahito (2020), este esquema de propiedad, dentro de su estrategia organizacional, opera como un mecanismo de conciliación entre los intereses individuales de los trabajadores y los de la compañía. En adición, dicho esquema de propiedad "se utiliza principalmente como un importante impulso para motivar la inversión concentrada en I+D e innovación" (Masahito, 2020: 44), lo que le permite a la compañía hacer coincidir los objetivos individuales con el desarrollo empresarial a largo plazo. Otro componente de su estrategia organizacional es la rotación constante del personal ejecutivo y directivo (con excepción del CEO), lo cual, si bien podría resultar ineficaz desde una perspectiva de continuidad de negocio, le ha servido para establecer un entorno fresco de oportunidades para la investigación e innovación.

Figura 1. Estrategias corporativas de Huawei

Fuente: elaboración propia con base en Masahito (2020).

A diferencia de otras compañías chinas, las cuales se caracterizan por establecer inversiones conjuntas (*joint-ventures*) con empresas extranjeras para adquirir conocimientos tecnológicos y capacidades de manufactura, Huawei ha preferido invertir sostenidamente más del 10% de sus ingresos anuales en I+D. En este sentido, se caracteriza por una estrategia de innovación abierta (Yan y Huang, 2022; Zang *et al.*, 2023) en la que busca reforzar sus vínculos con la academia a partir del *Huawei Innovation Research Program* (HIRP) establecido en 2010.

Por medio de HIRP, los ingenieros de la compañía han colaborado exitosamente con diferentes socios académicos de las mejores universidades para resolver complejos problemas técnicos en corto tiempo y de forma rentable. Además, la compañía fortalece su capacidad interna de innovación al fomentar el aprendizaje organizacional y la movilidad de talento para responder mejor a las oportunidades del mercado (Zang *et al.*, 2023), así como ofrecer incentivos para fomentar la lealtad de sus trabajadores, los cuales van desde salarios altos hasta instalaciones equipadas con lo necesario para promover su bienestar (dormitorios, cafeterías, un hospital, gimnasio, etc.) (Masahito, 2020)[2]. Sus esfuerzos de innovación se han reflejado en sus más de 120 000 patentes totales activas a finales de 2022.

La estrategia corporativa de expansión en el extranjero obedece al acceso que Huawei ha conseguido en mercados

2 En 2023, la empresa fue reconocida en México como "Top Employer". (https://www.huawei.com/mx/news/mx/2023/huawei-ha-sido-reconocida-como-top-employer-2023-en-mexico)

emergentes, donde ha buscado elevar los niveles tecnológicos. A partir de estos, la compañía ha intentado llegar a mercados europeos, Japón y Estados Unidos. De acuerdo con Masahito (2020), esta estrategia de expansión responde a un modelo de negocios inclusivo que incorpora al segmento social correspondiente a la base de la pirámide (aquellos con ingresos menores a 3000 dólares anuales). En adición, la compañía suele establecer equipos locales y capacitar a ingenieros locales para la operación en el extranjero y el mantenimiento de las filiales de Huawei (Guo y Liu, 2024).

Por otro lado, las buenas relaciones con clientes son fundamentales dentro del modelo de negocio de Huawei; la innovación de valor para el cliente se compone de un plan de comunicación y seguimiento de acciones con todos los clientes, el entendimiento de sus necesidades y la atención a sus quejas. De acuerdo con Zang *et al*. (2023), esto le sirve a Huawei para sostener relaciones estables en el largo plazo, al tiempo que se fortalece la confianza mutua.

La empresa ha pasado de revender equipos de conmutación a oficinas postales y ciudades pequeñas, a fabricar los suyos y extender el alcance de sus actividades hacia los cinco grandes grupos de negocios. La presencia global de la compañía en América, Europa, África y Asia, más los avances en el sector de información y telecomunicaciones, le han valido a Huawei una representación de empresa internacional de alta tecnología, en donde la preocupación por la ciberseguridad se ha traducido en una mayor apertura y transparencia de las acciones encaminadas para abordar los retos de extremo a extremo para los reguladores, gobiernos, clientes y consumidores. Además, se han emprendido otras acciones en términos de la gestión de riesgos en el procesamiento de datos, seguridad en las redes y métodos de protección de la privacidad, lo cual se refleja en un presupuesto, en los últimos cinco años, de 2000 millones de dólares para mejorar y potenciar plenamente las capacidades de la empresa en ingeniería de *software* (Huawei Technologies, 2019), y una inversión anual de cerca del 5% de su presupuesto de I+D en materia de ciberseguridad (Huawei Technologies, 2022a).

De tal forma, Huawei busca una integración de la seguridad en todas las fases de sus procesos internos, desde el análisis de requerimientos, diseño y la codificación, hasta las pruebas y la gestión del ciclo de vida. Al respecto, la compañía ha establecido un marco integral de ciberseguridad en el que se atienden cabalmente los requisitos de seguridad que pueden venir de los clientes, las leyes y las normas en vigor en cada país. Luego, estos requisitos se traducen en líneas de base de seguridad que son integradas a los procesos internos para ser ejecutadas repetidamente, controladas y auditables. En este contexto, a través de un departamento de auditoría interna, se comprueba si los demás departamentos han llevado a cabo las actividades de ciberseguridad según lo requerido y, finalmente, se invita a los directivos a participar en los debates y la toma de decisiones del Comité Global de Seguridad y Privacidad (GSPC), con el fin de plasmar sus ideas en resoluciones, estrategias y políticas que puedan servir de guía a todos los departamentos para garantizar la ciberseguridad (Huawei, 2019).

2. La estrategia de ciberseguridad de Huawei

La ciberseguridad se puede definir como el conjunto de prácticas que tienen por fin asegurar la protección de los sistemas críticos y la información confidencial ante cualquier posible ataque digital (Solleiro *et al.*, 2022). Los problemas relacionados con la seguridad de la información y la protección de datos personales, como aquellas amenazas que vulneran la integridad, la privacidad y la confidencialidad de los sistemas informáticos, son fenómenos que subyacen al rápido desarrollo del sector TIC. El refinamiento de los ciberataques, por ejemplo, está relacionado con el desarrollo de las tecnologías digitales intensivas en el uso de internet, el cual es el mayor medio de tráfico de datos[3] a escala global. En este sentido, y sin importar del tipo que sean (públicas o privadas), las organizaciones deben contar con una estrategia de ciberseguridad en la que establezcan tanto a los actores como a las medidas que habrán de emprenderse a fin de proteger la seguridad de sus sistemas.

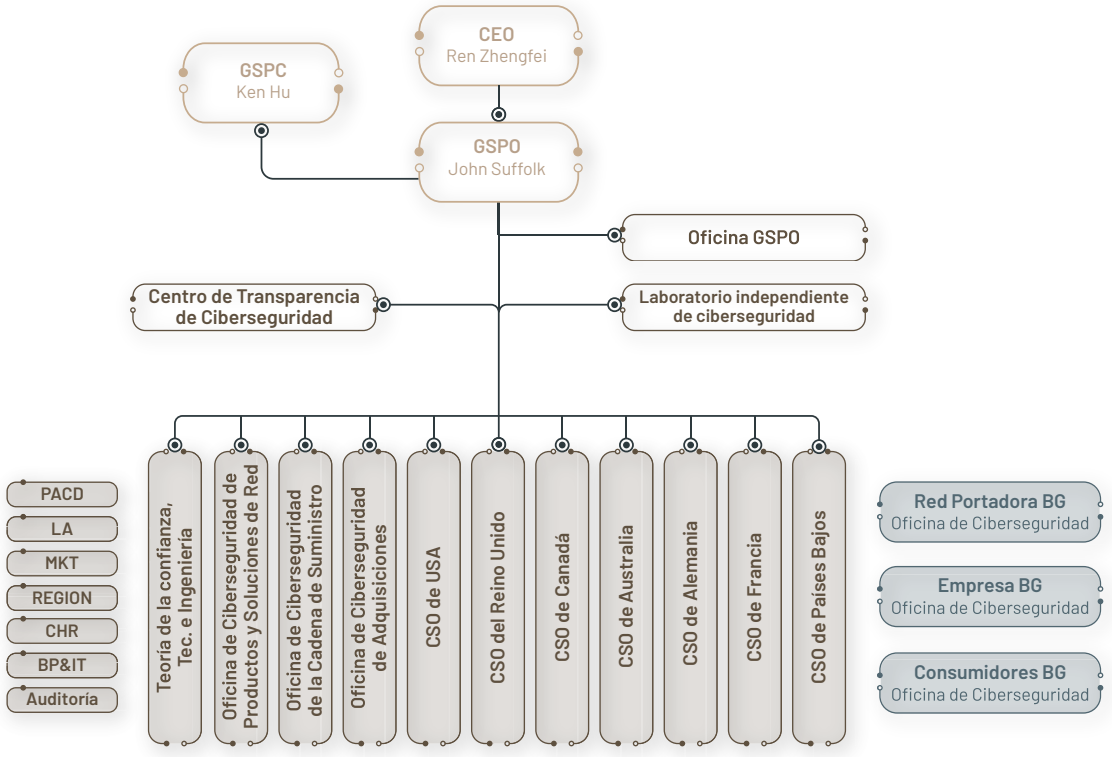
De acuerdo con Huawei (2023b), la estrategia de ciberseguridad de la compañía se basa en la adopción de un enfoque integral que va desde las fases de diseño, desarrollo (implementación de normas de codificación seguras) y prueba, hasta la construcción de centros internacionales de transparencia de ciberseguridad. En su último reporte anual, la compañía destaca que, durante los últimos cinco años, se ha mejorado y transformado todo el proceso de IPD, adoptando un enfoque de seguridad por diseño mediante la definición de requisitos de seguridad, la adopción de normas de codificación seguras en la fase de desarrollo, y la creación de nuevos modelos de ensayos de seguridad, como las pruebas de penetración, tolerancia a fallos y resistencia (Huawei Technologies, 2023b).

2.1 El enfoque integral de la ciberseguridad de Huawei

De acuerdo con DPL News (2022), Huawei cuenta con un ABC en materia de ciberseguridad, basado en *Assume Nothing* (No asumir nada), *Believe Nobody* (no creer en nadie) y *Check Everything* (verificar todo). Lo dicho refleja la importancia por la implementación de medidas de seguridad sólidas para proteger sus redes, sistemas y datos. Para verificar sus procesos, la compañía utiliza una variedad de técnicas que contemplan la revisión del código, las pruebas de penetración y el análisis de vulnerabilidades. Con el fin de no confiar en ninguna entidad externa para la protección de la seguridad, Huawei cuenta con su propio equipo interno de expertos en ciberseguridad (figura 2), el cual está encabezado por el comité global de ciberseguridad y protección a la privacidad (GSPC, por sus siglas en inglés) que responde directamente al CEO de la empresa, y establece la estrategia, el plan, la política, la hoja de ruta y la inversión en ciberseguridad (Huawei Technologies, 2019; Huawei Technologies 2024a).

3 Las estimaciones más recientes sitúan en una media de 2.5 quintillones de *bytes* de información generados diariamente a nivel mundial, de los cuales un aproximado de 90% circulan por medio de redes de banda ancha fija (Olaleye y Adusei, 2024).

Figura 2. Gobernanza de la ciberseguridad en Huawei



Fuente: adaptada de DPL News (2022).

Por otro lado, el Responsable Global de Ciberseguridad y Privacidad (GSPO) dirige un equipo de expertos para desarrollar estrategias de seguridad, estableciendo un sistema interno de garantía en ciberseguridad y apoyando a clientes y organizaciones externas a nivel global. La Oficina del GSPO es la organización central de la compañía encargada de identificar y resolver problemas relativos a la ciberseguridad, coordinando a los departamentos relacionados (I+D, *marketing* y ventas, gestión de la cadena de suministro, ingeniería, servicios técnicos, etc.) en la formulación de normas y acciones operativas que impulsen y apoyen la elaboración y ejecución de estrategias, así como la auditoría y el seguimiento. El Laboratorio Independiente de Ciberseguridad, que es la unidad de verificación, tiene la función de conducir pruebas de seguridad en profundidad y revisar el código (Portillo, 2020), sólo reporta al GSPO y al GSPC. Finalmente, las diversas oficinas de ciberseguridad (CSO) de las oficinas regionales y de cada país trabajan coordinadamente con el GSPO para identificar posibles cambios en los debidos procesos, "de modo que las estrategias y requisitos de ciberseguridad estén plenamente integrados en las operaciones empresariales" (Huawei Technologies, 2019: 30).

En este sentido, la compañía supervisa y mejora sus procesos internos por medio de la conducción de auditorías internas que, más tarde, son sometidas a acreditación de seguridad por organismos de diferentes países, tanto gubernamentales como independientes, y especialistas externos en materia de ciberseguridad.

Muestra de ello es el cumplimiento de la norma ISO 27001 (cuadro 1), que acredita al sistema de gestión de la información de Huawei como eficaz en la evaluación de riesgos. Otro ejemplo es la adopción de la metodología DevSecOps orientada a los servicios *cloud* y las capacidades técnicas relacionadas, lo cual permite garantizar la seguridad de extremo a extremo desde la I+D hasta el despliegue de los servicios (Huawei Technologies, 2024a).

La metodología de ciberseguridad de extremo a extremo implementada por Huawei, de acuerdo con DPL News (2022), se incorpora a doce procesos corporativos y módulos comerciales: **1)** Estrategia y gobernanza; **2)** Procesos, utilizando los mejores estándares y enfoques para la protección contra amenazas; **3)** Legislación y regulación, buscando que sus productos cumplan con los requisitos legales de los países en operación; **4)** Recursos humanos adecuados en puestos pertinentes para reducir las posibles debilidades internas en seguridad; **5)** I+D; **6)** Verificación de la seguridad; **7)** Gestión de proveedores; **8)** Manufactura y logística; **9)** Prestación segura de servicios, para garantizar que la instalación, el servicio y el soporte estén asegurados; **10)** Resolución de problemas, para garantizar que la tecnología de los clientes esté protegida; **11)** Trazabilidad, para rastrear hacia adelante y hacia atrás a cada persona y componente de cada proveedor en cada producto; y **12)** Auditoría.

Asimismo, la compañía ha comenzado la construcción de una comunidad de conocimiento sobre ciberseguridad y protección de la privacidad, con el objetivo de "facilitar el rápido intercambio y transferencia de conocimientos y mejorar la experiencia individual del personal que trabaja en ciberseguridad" (Huawei Technologies, 2023b: 78). Otros esfuerzos en línea con la sensibilización del personal en ciberseguridad han sido: **a)** la puesta en marcha de un campamento de formación en la materia, donde los trabajadores pueden compartir conocimientos y experiencias en procesos y escenarios empresariales mediante simulacros, juegos y conferencias de expertos; **b)** la creación de más de 160 cursos de capacitación en ciberseguridad y protección de la privacidad; y **c)** el lanzamiento de una campaña de concientización sobre la materia dirigida a todos los empleados.

En la misma línea, Huawei ha colaborado con el gobierno local y los transportistas de Malasia "en cultivo de talento y conciencia de seguridad cibernética" (Huawei Technologies, 2023b: 80), de lo cual ha recibido el premio a la Innovación Educativa en Ciberseguridad del año 2023. Por otro lado, la presencia de Huawei en Asia ha destacado por el establecimiento y puesta en marcha de laboratorios de innovación conjuntos, tanto con la industria energética nacional de Indonesia, como con el sector financiero chino.

2.2 La colaboración internacional para mejorar la ciberseguridad global

Con el fin de mejorar el entorno internacional de ciberseguridad, Huawei busca posicionarse como un actor global estratégico por medio del establecimiento de alianzas y marcos colaborativos de trabajo con diferentes organismos internacionales, tales como el Foro Económico Mundial y la Unión Internacional de Telecomunicaciones, con quienes ha colaborado para promover y desarrollar estándares de seguridad y mecanismos de verificación (Huawei Technologies, s.f.b) y, más recientemente, en 2024, con el Parlamento Latinoamericano y Caribeño (Parlatino), con quien busca colaborar en áreas relativas al desarrollo de infraestructuras digitales, creación de capacidades TIC, promoción de la inclusión digital y ciberseguridad (Huawei Technologies, 2024b).

Por otro lado, la apertura y puesta en marcha de diversos centros de transparencia de ciberseguridad en diferentes países se inscribe en la estrategia de ciberseguridad adoptada por la compañía. Están abiertos al público y sirven para comunicar, por medio de visitas guiadas, exposiciones, conferencias y talleres, las medidas, las prácticas y las tecnologías de Huawei en materia de seguridad. Actualmente, la empresa cuenta con siete de estos centros (Huawei Technologies, 2022c) en Dubái, Londres, Toronto, Milán, Múnich, Bruselas y Dongguan, China, este último es el más grande hasta la fecha. En adición, y de manera reciente, ha anunciado la creación del primer centro en territorio latinoamericano, el cual tendrá su sede en Panamá (Durán, 2024).

A finales de 2022, la compañía figuraba como miembro activo en cerca de 800 organizaciones de normalización, alianzas industriales, comunidades de código abierto (la Linux Foundation, por ejemplo) y diversas asociaciones académicas. Además, ha enviado cerca de 68 000 contribuciones a más de 200 organizaciones de normalización en el sector de las comunicaciones, de las cuales 12 000 corresponden al 2023 (Huawei Technologies, 2023b). En la figura 3 se exponen algunas de las principales colaboraciones que ha establecido Huawei en materia de ciberseguridad.

Figura 3. Colaboraciones internacionales de Huawei en materia de ciberseguridad

Fuente: elaboración propia con base en Huawei (2023b).

Dentro del 3GPP (asociación de siete organizaciones de desarrollo de estándares de telecomunicaciones), por ejemplo, Huawei ha contribuido a la creación de normas técnicas para la tecnología 5G-Advanced. Las colaboraciones de la compañía con organizaciones de estándares han versado sobre las redes 400G/800G (IEEE), las normas F5G Advanced (ETSI), y la normalización en la codificación y descodificación de imágenes basadas en inteligencia artificial (Comité Técnico Mixto, JTC, de ISO/IEC). A ello se agrega la presencia que ha tenido en el grupo de expertos de normalización en ciberseguridad IoT creado por la Asociación Española de Normalización (UNE, 2021), el cual fue presidido por Carlos Valderrama, asesor senior de ciberseguridad de la compañía.

Por otro lado, la compañía ha colaborado con organismos públicos como la Unión Internacional de Telecomunicaciones (UIT) con quien, en cooperación con el Centro de Seguridad Cibernética Regional Árabe (ITU-ARCC), ha lanzado el "Módulo de madurez de la estrategia de desarrollo de la industria de la ciberseguridad" (Teletimes, s.f.), el cual es un programa que proporciona una guía integral para las autoridades, las partes interesadas y los investigadores académicos para evaluar y mejorar sus capacidades de ciberseguridad. En España, país europeo donde la compañía tiene una presencia consolidada, ha participado en la elaboración del libro blanco de ciberseguridad en IoT, en colaboración con el Instituto Nacional de Ciberseguridad (Incibe). Por último, Huawei firmó recientemente un acuerdo de asociación estratégica con la empresa nacional de energía eléctrica de Indonesia (PLN) para la puesta en marcha de un laboratorio de innovación conjunto, desde el cual se busca explorar "las operaciones de red digital y las aplicaciones de ciberseguridad, y llevar a cabo innovaciones conjuntas en tecnologías como la detección de aplicaciones en profundidad y la fragmentación de la red" (Huawei Technologies, 2023b: 81).

En el campo industrial, las colaboraciones de Huawei abarcan desde la creación y prueba de soluciones de seguridad en redes 5G (China Mobile Zhejiang), la exploración y verificación de las capacidades de seguridad de la red informática (China Mobile Guizhou) para la protección contra el *ransomware*, hasta el establecimiento de un laboratorio de innovación conjunto en finanzas digitales (China CITIC Bank) para explorar aplicaciones de flujo libre de datos con confianza (DFFT). Entre las asociaciones académicas destaca la firma de un acuerdo de colaboración con la Universidad de León (ULE, España) en enero de 2023, del que resultó la creación y puesta en marcha de un Centro de Experiencias en Ciberseguridad en el campus de Vegazana.

2.3 Productos de ciberseguridad desarrollados por Huawei

Dentro de su amplio catálogo de productos y servicios, Huawei cuenta con una serie de soluciones relacionadas con la ciberseguridad para empresas (cuadro 1), entre las cuales destaca el sistema HiSec de detección de amenazas en tiempo real, con una tasa de detección del 99.9%. Recientemente, la compañía ha presentado la solución HiSec SASE, la cual se basa en la arquitectura integrada *"cloud-network-edge-device"* que permite gestionar las amenazas en cuestión de segundos desde la plataforma de análisis de seguridad Qiankun. En el lado de la red (*network*),

se emplea la tecnología de establecimiento de túneles dinámicos EVPN para implementar redes flexibles a gran escala. En el lado del dispositivo (*device*), se utiliza el motor de rastreo de origen de amenazas para detectar con mayor precisión virus de *ransomware* en dispositivos.

Por otro lado, Huawei Cloud ofrece servicios de seguridad en la nube (AAD, WAF, DEW y DBSS) certificados por la norma ISO 9001/TL 9000, lo que garantiza su calidad y rapidez.

Cuadro 1. Productos relacionados con ciberseguridad

Producto/Servicio	Descripción
USG9500	*Firewall* de nueva generación, de nivel terabit, diseñado para operadores de servicios cloud, centros de datos de gran tamaño y redes de campus empresariales a gran escala. Integra múltiples funciones de seguridad, como la traducción de direcciones de red (NAT), redes privadas virtuales (VPN), y sistema de protección contra intrusiones (IPS).
Sistemas de protección DDoS de la serie AntiDDoS1000	Dispositivos que ofrecen protección contra ataques de denegación de servicio distribuido (DDoS) que utilizan tecnología *big data* y admite modelado de más de 60 tipos de tráfico de red para una defensa integral.
Sistema de análisis avanzado de amenazas HiSec Insight	Realiza análisis de correlación multidimensional de datos masivos basados en un algoritmo de detección de inteligencia artificial. Detecta una amplia gama de eventos de amenazas a la seguridad en tiempo real, rastreando el comportamiento de ataque de toda la cadena de ataque de las amenazas persistentes avanzadas (APT), y recopila y almacena múltiples tipos de información de red, lo que ayuda a los usuarios a detectar amenazas, realizar análisis forenses y, en última instancia, eliminar amenazas.
Controlador de seguridad SecoManager	Controlador que proporciona gestión de políticas de seguridad en toda la red, y gestiona eficazmente las amenazas a gran velocidad, lo que mejora la capacidad de defensa.
Advanced Anti-DDoS (AAD)	Servicio orientado a servidores para la protección contra ataques DDoS, que puede bloquear el tráfico HTTP no autorizado, mejora la velocidad de acceso al sitio web vía almacenamiento del contenido estático en la memoria caché, y protege las aplicaciones web, móviles y API contra amenazas comunes.
Data Encryption Workshop (DEW)	Servicio de encriptación de datos en la nube y gestión de claves seguras (*Key Management Service*).
Web Application Firewall (WAF)	Emplea un motor de IA, decodifica más de 10 tipos de códigos y evita que las amenazas eludan los controles de seguridad. Además, permite que los datos sensibles (como cuentas y contraseñas) que aparezcan en los registros de ataques se puedan anonimizar.
Database Security Service (DBSS)	Servicio que adopta tecnologías de aprendizaje automático y *big data* para la protección de bases de datos en la nube, así como para auditarlas y detectar posibles comportamientos de riesgo.

Fuente: elaboración propia con base en DPL News (2022) y Huawei Technologies (s.f.c, 2023c).

2.3.1 La ciberseguridad 5G y la visión de una industria 5.5G

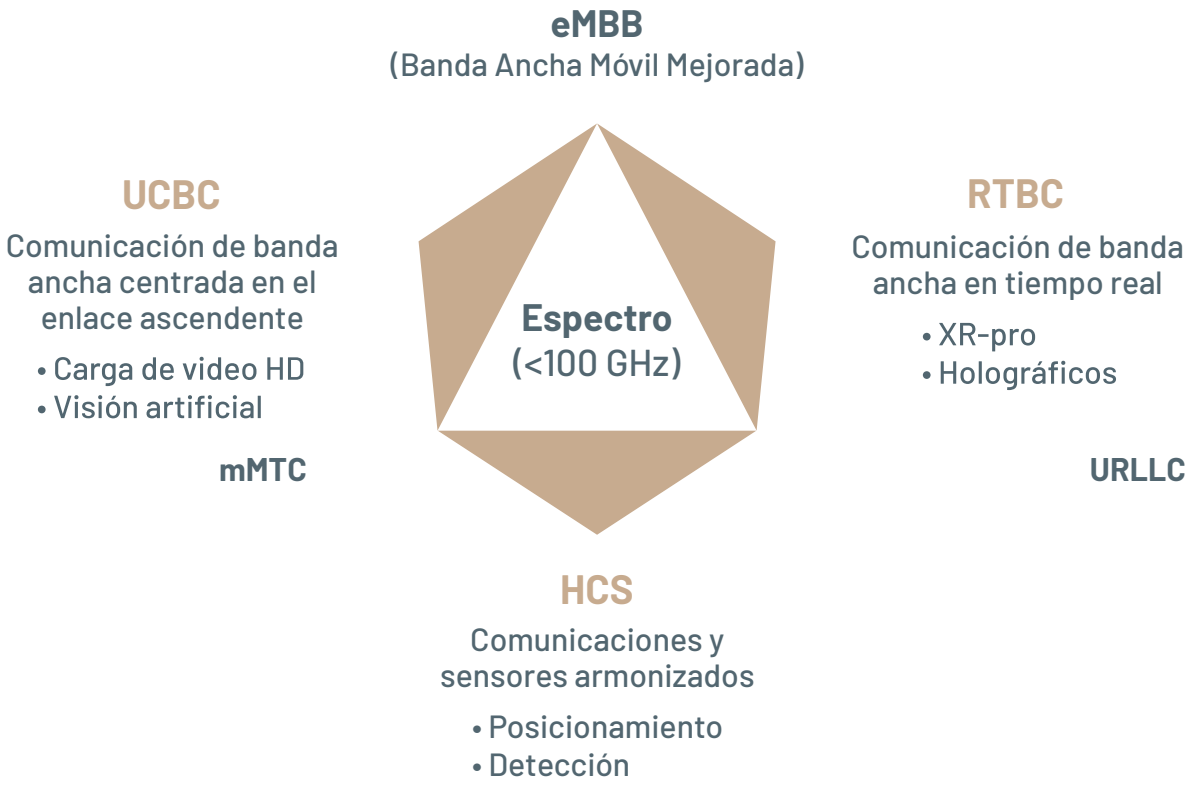
El rápido avance en la conexión de dispositivos mediante redes de banda ancha móvil trae consigo algunos asuntos de seguridad a los que Huawei ha enfrentado mediante los refuerzos a la seguridad de los estándares de la 5G, entre los cuales destacan (respecto a los propios de la 4G) la mayor seguridad de la interfaz aérea, la mayor protección de la privacidad del usuario, la mayor seguridad en itinerancia, y los algoritmos criptográficos mejorados (Huawei Technologies, 2021).

Respecto a la ciberseguridad, la 5G sigue los principios de diseño de defensa en profundidad, Zero-trust@5G y seguridad adaptativa. Lo anterior se traduce en medidas de seguridad multicapa para la protección de las amenazas externas (ataques y accesos no autorizados), la encriptación de la información para evitar su fuga en caso de ser robada y, para el caso de la confianza cero, un control de acceso dinámico mediante la autenticación de acceso, la autorización dinámica y la evaluación continua.

En un mundo hiperconectado, las redes 5G deben satisfacer los requisitos de una conectividad óptima en tres escenarios: **1)** Banda ancha móvil mejorada (eMBB): servicios que requieren un ancho de banda ultra alto, como el video de alta definición, realidad virtual y realidad aumentada; **2)** Comunicaciones masivas de tipo máquina (mMTC): conexiones de alta densidad, como el transporte inteligente, la industria 4.0 y la logística inteligente; y **3)** Comunicaciones ultra-fiables y de baja latencia (URLLC): servicios sensibles a la latencia, como la conducción autónoma/asistida o el internet de los vehículos (Huawei Technologies, 2021).

Huawei propone una visión de la industria 5.5G en la que define tres escenarios que mejoran los escenarios estándar de la 5G (figura 3): **1)** Comunicación de banda ancha centrada en el enlace ascendente (UCB) con un aumento de 10 veces en el ancho de banda de enlace ascendente, mediante lo cual se puede soportar cargas de gran volumen en escenarios de producción y fabricación para visión artificial (*machine vision*) y *IoT* de banda ancha masiva; **2)** Comunicación de banda ancha en tiempo real (RTBC) que admite un gran ancho de banda y muy baja latencia; y **3)** Comunicación y detección armonizadas (HCS) que amplían los límites de capacidad de las redes móviles y permiten el posicionamiento y la detección a nivel centimétrico.

Figura 3. Escenario 5.5G



Fuente: adaptado de Huawei Technologies (2021).

3. Cumplimiento de normas y certificaciones

Dentro de su estrategia de ciberseguridad, el cumplimiento de normas y estándares internacionales juega un papel fundamental en la construcción de un entorno de confianza digital (Huawei Technologies, s.f.d). En este sentido, Huawei se ha adherido al cumplimiento de una serie de requerimientos legales de nivel internacional. Destacan, por ejemplo: **a)** el cumplimiento de la ley de protección de datos personales en más de 170 países (México, Europa, Reino Unido, China, Argentina, Brasil, Japón, UEA, Sudáfrica, entre otros); y **b)** la obtención del Sello Europeo de Privacidad (EuroPriSe) por parte de Aspiegel Limited, filial propiedad de Huawei, para su servicio HUWEI ID en la Unión Europea y el Espacio Económico Europeo. El EuroPriSe que certifica la conformidad de los productos y servicios basados en TI con la normativa europea sobre privacidad y seguridad de datos.

De acuerdo con Huawei (2023b), a finales del 2023, la compañía había obtenido "más de 540 certificados de seguridad y privacidad. Solo en 2023, Huawei obtuvo 57 certificados de ciberseguridad" (Huawei Technologies, 2023b: 79). A continuación, en el cuadro 2 se exponen las acreditaciones en la materia más importantes con las que cuenta la compañía. Todas las certificaciones, excepto aquellas de orden regional, han sido otorgadas por organismos de alcance global.

Cuadro 2. Principales acreditaciones de Huawei en materia de ciberseguridad

Sistema de Gestión de la Información (SGI)	Protección de la información personal	Servicios en la nube	Certificaciones regionales	Otras certificaciones
ISO 27001	ISO/IEC 27018	CSA STAR	Classified Cybersecurity Portection of China's Ministry of Public Security	CC EAL6+
ISO/IEC 27701	ISO 29151:2017	NIST CSF	Certification for the Capability of Protecting Cloud Service User Data (China)	PCI DSS
	BS 10012:2017	ISO 20000-1:2018	Trusted Cloud Service (TRUCS, China)	

Continúa

	ISO 27017:2015	Trusted Information Security Assessment Exchange (TISAX, Europa)
	ISO 22301:2012	Singapore MTCS de nivel 3
	ISO 9001/TL 9000	OSPAR certification (Singapur)

Fuente: elaboración propia con base en Suffolk (2013) y Huawei Technologies (2022d, 2023b, 2023d).

Las diferentes certificaciones obtenidas tanto a nivel internacional como regional demuestran el compromiso adquirido por la compañía de garantizar la privacidad y la seguridad en el tratamiento de los datos personales. La norma ISO 27001, por ejemplo, certifica que Huawei cuenta con los requisitos necesarios para implementar y mejorar continuamente su sistema de gestión de la información, adoptando un método de evaluación periódica de riesgos, mientras que la norma ISO 27701 certifica que Huawei cuenta con un sistema integral de gestión de la protección de información personal en las fases de diseño e I+D (Huawei Technologies, 2020). En esta línea, la empresa se ha certificado en la protección de información de identidad personal en la nube (ISO 27018), contando para ello con objetivos de control y directrices seguras y confiables (ISO 29151:2017). Con la certificación BS 10012:2017, la cual proporciona un marco de mejores prácticas para un SGI alineado con los principios del Reglamento General de Protección de Datos de la Unión Europea (Huawei Technologies, s.f.e), la compañía garantiza contar con la capacidad necesaria para proteger la seguridad de los registros personales relacionados con individuos.

La certificación CSA STAR acredita a Huawei con la madurez tecnológica necesaria para garantizar una gestión integral de la seguridad en la nube de primera clase (Huawei Technologies, 2024a). Por su parte, el *Cybersecurity Framework* (CSF) del *National Institute of Standards and Technology* (NIST) consta de normas, directrices y buenas prácticas para la gestión de la ciberseguridad. Huawei es el primer proveedor de servicios en la nube de origen chino en obtener la certificación NIST CSF de más alto nivel (Huawei Technologies , s.f.f), lo cual la certifica en gestionar y reducir los riesgos de ciberseguridad a los que pueda enfrentarse su plataforma en la nube. A ello se añade la certificación ISO 9001/TL 9000, que certifica que la capacidad de Huawei Cloud para brindar servicios en la nube es de alta calidad y confiabilidad.

Respecto a las soluciones tecnológicas que suponen los servicios de computación en la nube (*cloud computing*), Huawei está certificada con las normas ISO 20000-1:2018 y 27017:2015 las cuales, respectivamente, garantizan tanto la implementación de sistemas eficaces de gestión de servicios de TI (Huawei Technologies, s.f.g) como la provisión de un entorno de nube confiable con los controles de seguridad de la información adecuados (Huawei Technologies, s.f.h). Por su parte, la certificación ISO 22301:2012 garantiza que Huawei puede ofrecer continuamente productos y servicios *cloud* maduros y de calidad (Huawei Technologies, s.f.i), dado

que la empresa está en condiciones de identificar, analizar y supervisar aquellos incidentes que perturben el entorno, minimizando las posibles pérdidas o costos de recuperación. A ello se añade la certificación de nivel 3 (la calificación más alta) del *Multi-Tier Cloud Security* (MTCS) de Singapur, el cual exige a los proveedores de servicios en la nube adoptar prácticas sólidas de gestión de riesgos y seguridad en la computación en la nube.

Huawei se asegura de cumplir con diferentes normas de carácter nacional, como la *Classified Cybersecurity Protection*, la *Certification for the Capability of Protecting Cloud Service User Data*, y la *Trusted Cloud Service*, todas de origen chino. Respectivamente, cada una de las certificaciones califica el nivel de ciberseguridad de la compañía; evalúa su capacidad para proteger los datos en la nube, desde la prevención previa al incidente y la protección durante el mismo, hasta el seguimiento posterior; y garantiza que la compañía cumple con el estándar más detallado para los datos de servicios en la nube. Por otro lado, Huawei aprobó las directrices de la Asociación de Bancos de Singapur por lo que, a través del informe de auditoría OSPAR, garantiza que la compañía es un proveedor de servicios de externalización (*outsourcing service provider*) confiable. En adición, la industria automovilística europea, a través de la *European Automobile Industry Security Data Exchange Association*, y la *Verband der Automobilindustrie*, ha reconocido a Huawei el cumplimiento de las normas de seguridad de la información y el intercambio de datos en la industria automotriz.

Finalmente, la compañía cuenta con el certificado de seguridad más alto disponible en el campo de los *kernels* (interfaz principal entre el *hardware* y los procesos ejecutados a través del *software*) de sistemas operativos. La certificación CC EAL6+ fue concedida en 2023 al *HongMeng Kernel*, el sistema operativo de los dispositivos electrónicos desarrollados por la compañía (desde celulares hasta pantallas), lo que supone un gran avance en garantizar la seguridad y la privacidad de sus productos (Huawei Technologies, 2023d). En adición, Huawei se ha comprometido con la protección de la información financiera relativa a los datos de los tarjetahabientes y sus datos sensibles de verificación mediante la obtención de la certificación *Payment Card Industry Data Security Standard* (PCI DSS) de nivel 1 (Huawei Technologies , s.f.j).

4. El Modelo de Responsabilidad Compartida de Huawei: protección de datos personales y el papel de los operadores

El control sobre la privacidad es un elemento de vital importancia para Huawei. En el caso de los productos de consumo que utilizan los servicios móviles de Huawei (HMS por sus siglas en ingles), por ejemplo, solamente se recolecta información personal de todo tipo (fotografías, contactos, registros telefónicos, correos electrónicos, sitios web visitados con frecuencia) de acuerdo con las leyes y regulaciones vigentes de los países en los que mantienen operación, y con el consentimiento informado del usuario. Para evitar que se puedan identificar individuos con base en sus datos personales, los HMS asignan identificadores (ID) aleatorios cuando comparte datos con los desarrolladores (Huawei Technologies, 2020).

Huawei es, en palabras de Tao, Cremer y Chumbo (2018), un contratista de ingeniería de telecomunicaciones que posee la capacidad de ofrecer en ciertos proyectos "un poderoso arsenal de las llamadas soluciones "llave en mano" (TK, por sus siglas en inglés), que han ayudado a contribuir al éxito de sus clientes en el mercado global" (Tao, Cremer y Chumbo, 2018: 93).

Las soluciones TK refieren, en síntesis, a que los clientes confieren, bajo acuerdos comerciales con la compañía, las responsabilidades del diseño de la red, obras civiles para adaptación de sitios, la adquisición del sitio a nombre del operador, los servicios de instalación, el transporte de equipos y las pruebas de red, así como de la preparación completa del sistema. En este sentido, Huawei junto con el operador definen las consideraciones para que la responsabilidad en la seguridad de la información, protección a la privacidad y otras obligaciones de las leyes aplicables se cumplan en beneficio de la compañía y sus clientes. Para el caso de la distribución de responsabilidades en los escenarios y entorno de nube publica, Huawei establece su Modelo de Responsabilidad Compartida (figura 4), definido con base en las prácticas generalizadas para la nube pública de toda la industria.

Figura 4. Modelo de Responsabilidad Compartida de Huawei Cloud

Fuente: adaptada de Huawei Technologies (2024a).

Huawei Cloud, la división de la compañía especializada en servicios en la nube, es responsable de la infraestructura física de sus centros de datos, de los servicios que proporciona y de las funciones de seguridad integradas en ellos (recuadros cafés). Por su parte, los clientes (*tenants*, recuadros azules) son responsables de "personalizar las configuraciones y operar la red virtual, la plataforma, las aplicaciones, los datos, la gestión, la seguridad y otros servicios cloud a los que se suscriben en Huawei Cloud" (Huawei Technologies, 2024a: 8). Esto, desde la perspectiva de la compañía, les confiere la responsabilidad de aquellas configuraciones de seguridad que sean necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Los operadores (o prestadores de servicios móviles), son compañías generalmente privadas con las que contratan los usuarios finales, y se pueden entender como organizaciones comerciales que tienen una concesión para la transmisión de datos vía su red pública de telecomunicaciones (Polo, 2020). En este sentido, los usuarios finales que contratan un servicio de telefonía o acceso a internet, por ejemplo, interactúan muchas veces de manera inconsciente con un operador que requiere y recopila los datos de tráfico necesarios para el procesamiento de dicha comunicación (número de teléfono, fecha y hora de la llamada, duración de la llamada, etc.). Mientras que a los fabricantes les corresponde la adopción de medidas de seguridad para la protección de datos y de la privacidad en el diseño de sus productos, así como la protección de la información personal identificable en la web para el caso de sus servicios en la nube, en el que la compañía cuenta con ciertas certificaciones.

De acuerdo con la legislación en diferentes países, la protección de los datos de los usuarios es la obligación de la organización o entidad que determina la recolección de datos y su procesamiento, que son típicamente los operadores, en donde se les asigna la responsabilidad de: **1)** Mantener niveles adecuados de seguridad y confidencialidad de los datos de los titulares; **2)** Informar acerca de posibles riesgos o medidas a adoptar, mediante cláusulas contractuales, ante una posible violación de la seguridad pública de las comunicaciones electrónicas; y **3)** Cumplir con todas las disposiciones establecidas en la ley nacional de protección de datos personales (Unidad Reguladora y de Control de Datos Personales, 2018).

En el caso de las redes móviles de última generación (ejemplo: 5G), la industria también ha trabajado para generar marcos para su despliegue seguro. Uno de los más consolidados es el Esquema de Garantía de la Seguridad de Equipo (*NESAS-GSMA Network Equipment Security Assurance Scheme*). La Asociación para el Sistema Global de Comunicación Móvil (GSMA, por sus siglas en inglés) ha desarrollado protocolos y estándares para la tecnología móvil, entre ellos su base de conocimientos para ciberseguridad que es seguida por los principales actores de la industria a nivel global. NESAS aporta un marco para garantizar la seguridad, lo cual eleva la confiabilidad y la confianza en el equipamiento de redes.

El objetivo del esquema es auditar y examinar a los proveedores de equipo y sus productos, de acuerdo con una línea de base que constituye el estándar mínimo a cumplir, de tal manera que los operadores de redes móviles puedan verificar la conformidad de los equipos con el estándar deseado. También se cuenta con un protocolo de pruebas, conocido como Especificaciones de Garantía de Seguridad (SCAS, por sus siglas en inglés), mediante las cuales los procesos de desarrollo y gestión del ciclo de vida de productos son auditados, a partir de pruebas de seguridad definidas por el 3GPP (*3rd Generation Partnership Project -Proyecto Asociación de Tercera Generación*) (3GPP, s.f.)[4]. Las pruebas relativas a esos requisitos permiten medir objetivamente el nivel de seguridad de los productos de la red. Como se ha mencionado, este esquema ha sido definido por expertos de la industria trabajando con GSMA y 3GPP, que es una colaboración de grupos de asociaciones de telecomunicaciones, para asentar las especificaciones de un sistema global de comunicaciones de tercera generación.

Huawei, como proveedor global de equipo de telecomunicaciones, se ha sometido a las auditorías de NESAS y SCAS. Huawei fue el primer proveedor en pasar el esquema de seguridad NESAS de GSMA, lo que indica que sus productos y procesos de desarrollo y ciclo de vida cumplen con los requisitos de seguridad y confiabilidad del esquema. También fue el primer proveedor en pasar las pruebas de seguridad SCAS definidas por 3GPP, lo que garantiza que sus productos cumplen con los requisitos de seguridad y confiabilidad de las especificaciones de seguridad de 3GPP (Huawei Technologies, 2021b).

4 Las especificaciones incluyen tecnologías para las comunicaciones por celular (equipo de acceso por señal de radio, capacidades de red y servicio) que aportan una descripción completa de los sistemas para comunicaciones móviles (https://www.3gpp.org/about-us)

El proceso de auditoría de NESAS (GSMA, s.f.) incluye una evaluación del nivel de cumplimiento de los requisitos de seguridad definidos por GSMA para el desarrollo de productos y la gestión de su ciclo de vida. El proceso de auditoría no es solamente mediante una revisión documental, pues hay una inspección por parte de un equipo especializado para verificar que los controles de seguridad se realicen efectivamente en la práctica. Las empresas proveedoras de equipo y tecnología que aprueban la auditoría son consideradas confiables.

Conclusiones

Huawei ha destacado por sus estrategias corporativas enfocadas en la investigación y desarrollo de tecnologías, nuevas teorías, aplicación y obtención de patentes esenciales, en las tecnologías de la información y comunicaciones, así como en su compromiso con las energías sustentables, las cuales le han permitido mantenerse a la vanguardia en el mercado mundial como uno de los mayores proveedores de infraestructura y servicios de telecomunicaciones. Consciente de los peligros que suponen los ataques digitales y las violaciones a la privacidad y confidencialidad de los datos, la compañía ha adoptado una estrategia de ciberseguridad integral que se caracteriza por:

1. Una estructura vertical de gobernanza que coordina, desde la GSPC, toda la estrategia a implementar en coordinación con los demás departamentos.
2. Una metodología de extremo a extremo que se incorpora a doce procesos corporativos y módulos comerciales, desde el diseño y el desarrollo, hasta la trazabilidad.
3. La conducción de auditorías internas, externas y de clientes que, más tarde, serán sometidas a acreditación de seguridad por organismos internacionales especializados en ciberseguridad.
4. La construcción de una comunidad interna de conocimiento sobre ciberseguridad y protección de la privacidad, dirigida a los empleados de la compañía.
5. Una estrategia de comunicación continua, fundamentada en la apertura de diversos centros de transparencia de ciberseguridad.
6. Una constante colaboración internacional con organismos de estandarización en el sector de telecomunicaciones, organismos públicos, asociaciones de la industria y organizaciones académicas.

En suma, la cuestión de la ciberseguridad como un asunto de responsabilidad compartida se identifica en las acciones de Huawei en el que, a través de gobernanza, gestión de riesgos, adaptación de controles de seguridad en los procesos de negocio y las diversas certificaciones, acreditan a la compañía en la provisión de productos y servicios que integran medidas de seguridad, y también para contribuir a las medidas de control para el cumplimiento de la ley de protección de datos personales por parte de los operadores.

Referencias

3GPP. (s.f.). About 3GPP. https://www.3gpp.org/about-us

Asociación Española de Normalización [UNE]. (2021). UNE crea un grupo de expertos de normalización en ciberseguridad IoT. https://www.une.org/la-asociacion/sala-de-informacion-une/noticias/impulso-a-la-ciberseguridad-iot

Ding, R. (2018). From Lone Heroes to Heoric Teams. En Tao, T. y Zhifeng, Y. [Eds.], *Explorers. Huawei Stories,* pp. 18-29. Londres: LID Publishing Limited.

DPL News. (2022). *Huawei: transparencia ante el mundo y cuidado end to end para reducir el riesgo a cero.* https://dplnews.com/wp-content/uploads/2022/05/Huawei-transparencia-ante-el-mundo-y-cuidado-end-to-end-para-reducir-el-riesgo-a-cero-ciberseguridad.pdf

Durán, S. (7 de junio de 2024). Huawei abrirá un centro de transparencia y ciberseguridad en Panamá este 2024. *DPL News.* https://dplnews.com/huawei-centro-de-transparencia-y-ciberseguridad-panama/

GSMA. (s.f.). GSMA Network Equipment Security Assurance Process Audit in detail. https://www.gsma.com/solutions-and-impact/technologies/security/nesas-process-audit/

Guo, Z. y Liu, Z. (2024). How Could Huawei Grow to the Largest Telecommunication Service Providing Company in Burma. *Business Administration and Management*, *6*(1), 11-16. DOI:10.18282/bam.v2i2.1369

Huawei Technologies. (2019). Huawei´s Position [Paper on Cyber Security]. https://www-file.huawei.com/-/media/corporate/pdf/public-policy/huaweis_position_paper_on_cybersecurity.pdf

Huawei Technologies. (2020). Huawei Mobile Services (HMS). Security Technical [White Paper]. https://consumer.huawei.com/content/dam/huawei-cbg-site/common/campaign/privacy/whitepaper/huawei-mobile-services-(hms)-security-technical-white-paper-v1.0.pdf

Huawei Technologies. (2021). Huawei 5G Security [White Paper]. https://www-file.huawei.com/-/media/corp2020/pdf/trust-center/huawei-5g-security-white-paper-2021-en.pdf?la=en

Huawei Technologies. (2021b). Huawei 5GC: The First to Pass 3GPP SCAS Testing and then Passes the GSMA NESAS Evaluation. https://www.huawei.com/en/news/2021/5/gsma-scas-neasa

Huawei Technologies. (2022a). No todo lo que escucha es verdad. Le invitamos a conocernos [Sección Noticias de Huawei]. https://www.huawei.com/mx/facts

Huawei Technologies. (2022b). A quién le pertenece Huawei [Sección Preguntas y respuestas]. https://www.huawei.com/mx/facts/question-answer/who-owns-huawei

Huawei Technologies. (2022c). Ken Hu, Presidente rotativo de Huawei: La confianza digital se basa en normas y hechos verificables. https://www.huawei.com/mx/facts/voices-of-huawei/ken-hu-digital-trust-is-built-on-standards-and-verifiable-facts

Huawei Technologies. (2022d). Huawei Cloud. Financial Cyber Security [White Paper]. https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/HUAWEI_CLOUD_Financial_Cyber_Security_White_Paper.pdf

Huawei Technologies. (17 de enero de 2023a). Huawei ha sido reconocida como Top Employer 2023 en México. https://www.huawei.com/mx/news/mx/2023/huawei-ha-sido-reconocida-como-top-employer-2023-en-mexico

Huawei Technologies. (2023b). 2023 *Annual Report*. https://www.huawei.com/en/annual-report

Huawei Technologies. (6 de agosto, 2023c). La seguridad en la nube con Huawei CLOUD | Certificación HCIA-Cloud Service. https://forum.huawei.com/enterprise/es/servicio-document-database-dds-certificaci%C3%B3n-hcia-cloud-service/thread/667241508786552832-667212887476809728

Huawei (14 de agosto, 2023d). Huawei tiene certificación de seguridad de más alto nivel en sistemas operativos de dispositivos inteligentes. PR Newswire. https://www.prnewswire.com/news-releases/huawei-tiene-certificacion-de-seguridad-de-mas-alto-nivel-en-sistemas-operativos-de-dispositivos-inteligentes-301899813.html

Huawei Technologies. (2024a). Huawei Cloud Security [White Paper]. https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/SecurityWhitepaper_intl_en.pdf

Huawei Technologies. (2024b). Firma de acuerdo de cooperación entre Huawei y Parlatino fortalecerá la inclusión digital. https://www.huawei.com/mx/news/mx/2024/mou-huawei-y-parlatino-fortalecera-la-inclusion-digital

Huawei Technologies. (s.f.a). Investigación e innovación. https://www.huawei.com/mx/corporate-information/research-development

Huawei Technologies. (s.f.b). Huawei Cyber Security Transparency Centre. Bruselas. https://www.huawei.com/-/media/CORPORATE/PDF/trust-center/huawei-cyber-security-transparency-centre-brochure-en

Huawei Technologies. (s.f.c). Network Security Products. https://e.huawei.com/en/products/security

Huawei Technologies. (s.f.d). Declaración sobre el establecimiento de un sistema de aseguramiento de la ciberseguridad global. https://www.huawei.com/mx/declarations/cyber-security

Huawei Technologies. (s.f.e). Huawei Cloud. BS 10012. A best practice framework for personal information management system. https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/bs-10012.html

Huawei Technologies. (s.f.f). Huawei Cloud. NIST Cybersecurity framework. An internationally recognized system for security assessment. https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/nist.html

Huawei Technologies. (s.f.g). Huawei Cloud. ISO/IEC 20000. The international standard for IT service management. https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/iso-20000-1.html

Huawei Technologies. (s.f.h). Huawei Cloud. ISO/IEC 27017. The international standard and guidelines for information security controls applicable to the provision and use of cloud services. https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/iso-27017.html

Huawei Technologies. (s.f.i). Huawei Cloud. ISO/IEC 22301. An international standard for business continuity management systems. https://www.huaweicloud.com/intl/es-us/securecenter/compliance/compliance-center/iso-22301.html

Huawei Technologies. (s.f.j). PCI DSS. The world´s most widely recognized and most stringent certification for financial institutions. https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/pci-dss.html

Masahito, A. (2020). Innovative Chinese Firms: A Case Study of Huawei´s Corporate Strategies and the Impact of US-China High-Tech War. En Kimura Koichiro [Ed.], *Innovation in East Asia*, [BRC Research Report], pp. 34-51. Bangkok: Bangkok Research Center.

Olaleye, S. y Adusei, A. (2024). The new reality of data economy and productization: A conceptual paper. *Finnish Business Review.* https://oulurepo.oulu.fi/handle/10024/50470

Polo, A. (2020). Telecomunicaciones y protección de datos: interconexiones de redes, datos de tráfico y conservación de datos. *Revista Vasca de Administración Pública,* 116, 213-243.

Portillo, M. (2020). *Huawei: Security Assurance and Transparency. Vision and Strategy.* https://www.cepal.org/sites/default/files/events/files/presentacion_martin_portillo.pptx_.pdf

Solleiro, J. L., Castañón, R., Guillén, A., Hernández, T. Y. y Solís, N. (2022). *Vigilancia tecnológica en Ciberseguridad.* Boletín Núm. 1. https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

Suffolk, J. (2013). *Cyber Security Perspectives. Making cyber security a part of a company´s DNA.* https://www.nist.gov/system/files/documents/2016/09/16/huawei_rfi_white_paper.pdf

Tao, T., De Cremer, D. y Chumbo, W. (2018). *Huawei. Liderazgo, Cultura y Conectividad.* México: LID Publishing Limited.

Teletimes. (s.f.). ITU-ARCC and Huawei launch the World's First Arab Cybersecurity Industry Development Strategic Maturity Model: A new guide to strengthen cybersecurity in Arab Region. https://teletimesinternational.com/2023/itu-arcc-and-huawei-launch-the-worlds-first-arab-cybersecurity-industry-development-strategic-maturity-model-a-new-guide-to-strengthen-cybersecurity-in-arab-region/

Unidad Reguladora y de Control de Datos Personales (2018). *Manejo de datos personales en operadores de telecomunicaciones.* https://www.opp.gub.uy/sites/default/files/inline-files/5MANEJODEDATOSPERSONALESENOPERADORESDETELECOMUNICACIONES.pdf

Verjan, R. M. (26 de julio de 2023). Huawei incrementa inversión en Investigación y Desarrollo. https://mundoejecutivo.com.mx/actualidad/huawei-incrementa-inversion-en-investigacion-y-desarrollo/

Wang, C., Chen, M., Wang, Q., Fang, Y. y Qiu, L. (2024). New product development paradigm from the perspective of consumer innovation: A case study of Huawei´s integrated product development. *Journal of Innovation and Knowledge*, 9(2). DOI: 10.1016/j.jik.2024.100482

Wu, X., Murmann, J. P., Huang, C. y Guo, B. (2020). *Huawei's R&D Management Transformation.* Cambridge University Press.

Yan, X. y Huang, M. (2022). Leveraging university research within the context of open innovation: The case of Huawei. T*elecommunications Policy*, 46(2). c

Zang, S., Hong, R., Pan, X. y Wang, H. (2023). Field Transitions, Value Innovation, and Firm's Leapfrogging: The Case of Huawei (1987-2022). http://dx.doi.org/10.2139/ssrn.4561145

Cuidado de la edición: Norma Solís Mérida
Apoyo en la edición: Eréndira Velázquez Campoverde

Dirección de diseño
Mariana I. Barajas Tinoco

Diseño
Mariana García Delgado
María Fernanda Gasca Alcántara