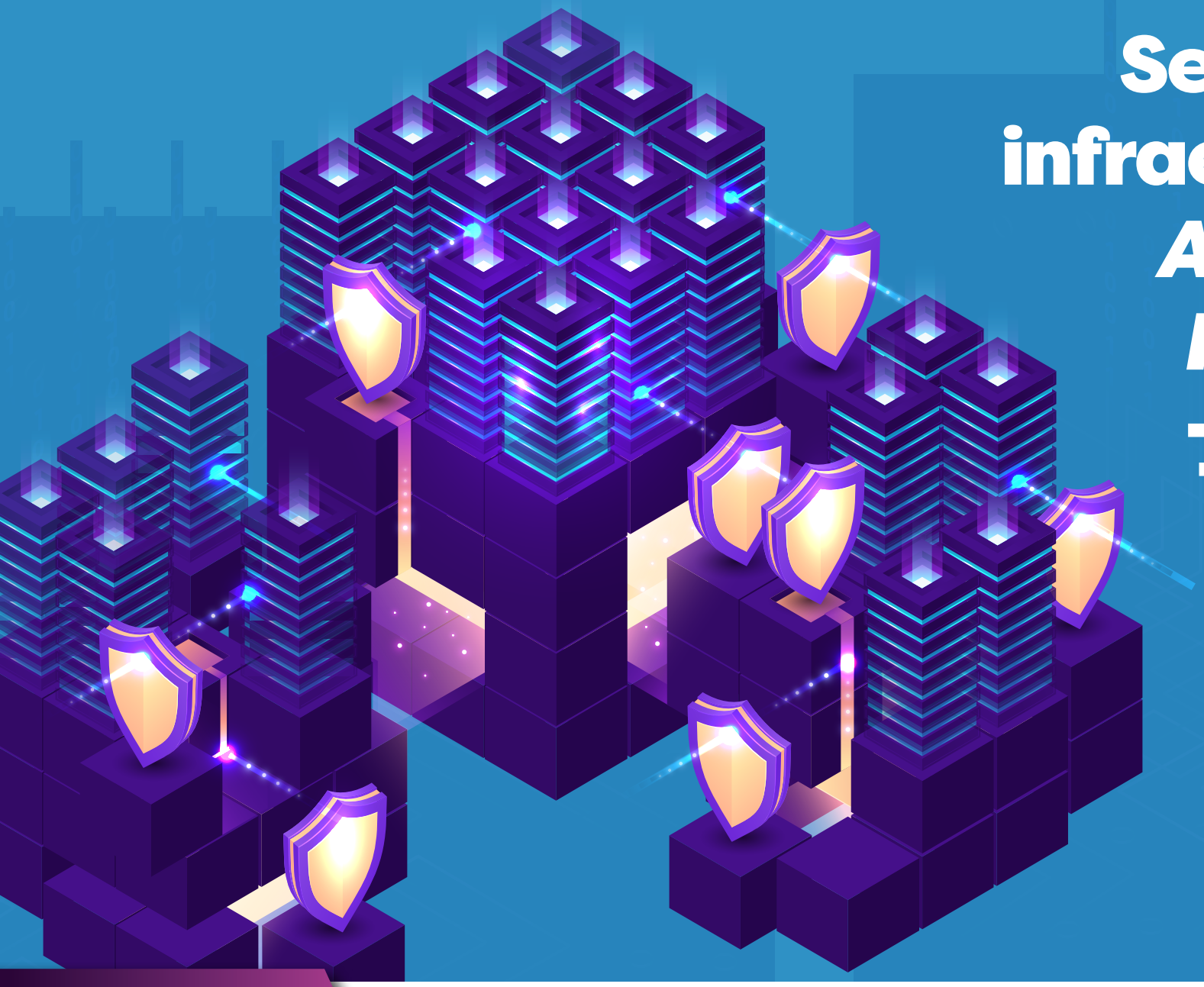

Seguridad de infraestructuras *Access Point Name* (APN)

Mejores Prácticas en Ciberseguridad

B.02

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Códigos JEL: D82, H12, K24, L86, L96, M15, O20, O21, O33

Palabras clave: ciberseguridad, amenazas cibernéticas, riesgos cibernéticos, seguridad de sistemas, seguridad de dispositivos, telefonía celular, infraestructura celular, redes celulares, Access Point Name, nombre del punto de acceso

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *Recomendaciones de implementación: seguridad de infraestructuras APN (Access Point Name)*.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la División de Capacidad Institucional del Estado (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/pages/apn.** Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *startups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Grupo de Datos y Gobierno Digital (DDG) de la División de Capacidad Institucional del Estado (ICS) del BID, disponible en: **https://www.iadb.org/es/quienes-somos/topicos/modernizacion-del-estado/datos-y-gobierno-digital**.

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

Listado de siglas

Sigla	Definición
APN	*Access Point Name*
BTS	Estación transceptora base
DoS	Denegación de servicio
eSIM	SIM integrada
IMEI	Identidad internacional de equipo móvil
IMSI	Identidad internacional de suscriptor móvil
IP	Protocolo de Internet
LAN	Red de área local
LTE	Evolución a largo plazo
MITM	Ataque de intermediario
MMS	Servicio de mensajería multimedia
QR	Código de respuesta rápida
SIGINT	Inteligencia de señales
SIM	Módulo de identificación de suscriptor
SMS	Servicio de mensajes cortos
VRF	Enrutamiento y reenvío virtual

Introducción

Nombre del punto de acceso, del inglés *Access Point Name* (APN), es un término colectivo para un grupo de configuraciones de trabajo aceptadas cuya finalidad es permitir que el proveedor de telefonía celular (u otra parte autorizada) supervise y controle la actividad de un activo cibernético (como un teléfono móvil) vinculado a la infraestructura de la red celular.

Para simplificar este asunto, aunque no sea lo suficientemente preciso, la infraestructura APN puede considerarse como una especie de red de área local virtual (VLAN, por sus siglas en inglés) o un enrutamiento y reenvío virtual (VRF, por sus siglas en inglés)[2] que el proveedor de tecnología celular configura en la red celular y, según sea necesario, aplica una lista de control de acceso (ACL, por sus siglas en inglés). El proveedor puede remitir a distintos grupos destinatarios a una infraestructura APN específica según diferentes parámetros (por ejemplo, la asignación del número de identidad internacional de suscriptor móvil [IMSI, por sus siglas en inglés][3] y el módulo de identificación de suscriptores [SIM, por sus siglas en inglés][4] a una organización en particular),[5] siendo habitual que el proveedor ofrezca a todos sus clientes la posibilidad de usar una infraestructura APN predeterminada.

Después de la configuración de la infraestructura APN por parte del proveedor, el usuario puede aplicar manualmente los ajustes de configuración necesarios para vincularse al APN o, alternativamente, pueden aplicarse los ajustes de configuración necesarios al activo cibernético mediante el uso de un mecanismo automatizado que el proveedor ofrezca a sus clientes. De esta forma, un activo cibernético que se conecte a la estación transceptora base (BTS, por sus siglas en inglés) tras completar con éxito un proceso de autenticación, será redirigido al APN que le corresponda.

Por otra parte, cabe destacar que existen casos en los que los proveedores celulares permiten que las señales de otros proveedores utilicen su red celular, dirigiendo el tráfico al proveedor correspondiente.

A nivel de ciberseguridad, las organizaciones que utilicen una red celular pueden reducir la superficie de ataque mediante el uso de una infraestructura APN privada.

Asimismo, una infraestructura APN privada puede brindar servicios de valor añadido a la organización, como el uso de números acortados entre usuarios de esta, y además los activos cibernéticos que formen parte de la infraestructura APN privada pueden recibir un nivel de servicio más alto en caso de producirse una sobrecarga o un incidente de emergencia que afecte a la infraestructura celular.

En el cuadro 1 se presenta una visión de conjunto de las generaciones de infraestructura celular.[6]

2. VRF es una tecnología para implementar instancias independientes de tablas de enrutamiento en equipos de comunicación, lo que permite una separación lógica entre distintas redes (red de área local/red de área amplia [LAN/WAN, por sus siglas en inglés]), así como la aplicación de ajustes de configuración específicos a diferentes clientes que compartan la misma infraestructura física.
3. La IMSI es un campo de 64 bits basado en tres componentes: (i) código de país móvil (MCC, por sus siglas en inglés), (ii) código de red móvil (MNC, por sus siglas en inglés) e (iii) identidad de suscriptor móvil (MSIN, por sus siglas en inglés). El IMSI se almacena en la tarjeta SIM y en el registro de ubicación de hogar (HLR, por sus siglas en inglés) junto al proveedor celular. *Fuente:* IMEI.info, **https://www.imei.info/imsi/.**
4. Cada tarjeta SIM cuenta con un número identificador único conocido como identificador de tarjeta de circuito integrado (ICCID, por sus siglas en inglés).
5. El mercado ofrece alternativas a la tecnología SIM tradicional, como SIM integrada (eSIM, por sus siglas en inglés) y SIM virtual.
6. Esta visión de conjunto es general, no exhaustiva y abstracta por razones de comodidad.

Cuadro 1. Generaciones de infraestructura celular

Generación		Descripción
1.	1G	El desarrollo de la primera generación dio comienzo a finales de 1970 y fue implementada por primera vez en 1987. Esta generación se basa en una configuración de trabajo analógica y usa una frecuencia de 30 kHz, lo que proporciona un ancho de banda de 2 kilobits por segundo (kbps).
2.	2G	Esta generación incluye una serie de tecnologías fundamentales y se originó en 1991: i. Sistema global para comunicaciones móviles (GSM, por sus siglas en inglés): un estándar que une los protocolos de comunicación celular, cuya principal innovación es la transición a una configuración de trabajo digital. ii. Acceso múltiple por división de código (CDMA, por sus siglas en inglés): un estándar que regula los procesos de recepción/envío de información de manera simultánea por una serie de consumidores que comparten el mismo rango de referencia. iii. Tecnologías digitales para superar el desvanecimiento (*fading*) y corregir errores. iv. Estándar de recepción/envío de mensajes por medio de servicio de mensajes cortos (SMS, por sus siglas en inglés).
3.	3G	Esta generación incluye una serie de tecnologías fundamentales: i. La arquitectura de sistema universal de telecomunicaciones móviles (UMTS, por sus siglas en inglés), que se originó en 2003 y proporciona la capacidad de transferir contenidos en una infraestructura celular, como la transmisión de video. Además, esta arquitectura se basa en un servicio internacional, lo que ha ampliado las capacidades de intercambio de información entre consumidores que no comparten la misma área geográfica. Una ventaja complementaria de esta tecnología es la capacidad del proveedor de tecnología celular de incrementar la capacidad de la infraestructura. Ancho de banda 384 kbps en movimiento y 2 megabits por segundo (Mbps) en reposo. ii. En 2006 se lanzó la tecnología *High-Speed Downlink Packet Access* (HSDPA), que aumentaba el ancho de banda a 42 Mbps. iii. Evolución a largo plazo (LTE, por sus siglas en inglés) es la última versión y ha aumentado el ancho de banda y la capacidad de la infraestructura. En ocasiones, esta se clasifica erróneamente como 4G.
4.	4G	Esta generación incluye una serie de tecnologías fundamentales y se originó en 2012: i. LTE Advanced o LTE+, que permiten transferir contenidos en "tiempo real" en la infraestructura celular, como la transmisión de vídeo, y recibir ancho de banda de 150 Mbps. ii. Voz por LTE (VoLTE, por sus siglas en inglés), que permite realizar llamadas telefónicas en una infraestructura 4G.
5.	5G	Esta generación es la versión más actualizada hasta el momento y permite recibir un ancho de banda de 1 gigabit por segundo (Gbps), y una latencia baja de aproximadamente 1–3 ms. Además, el método de señalización (*signaling*) en esta versión está basado en el protocolo de Internet (IP, por sus siglas en inglés).

En el cuadro 2 se muestra una división de las configuraciones de trabajo comunes al utilizar una APN.

Cuadro 2. Configuraciones de trabajo comunes en APN

	Configuración de trabajo	Descripción
1.	Infraestructura APN pública	El activo cibernético está conectado a una red de comunicación que permite de forma predeterminada la conectividad a servicios de datos públicos (como Internet) y servicios de voz. En este caso, el operador no limita la conectividad entre los distintos activos cibernéticos.
2.	Infraestructura APN pública que aplica un aislamiento lógico entre los activos cibernéticos	El activo cibernético está conectado a una red de comunicación que permite de forma predeterminada la conectividad a servicios de datos públicos (como Internet) y servicios de voz. En este caso, el operador limita la conectividad entre los distintos activos cibernéticos en función de sus necesidades.
3.	Infraestructura APN privada	El activo cibernético está conectado a una red de comunicación que, según decida la organización, permite la conectividad a servicios de datos públicos (como Internet) y/o servicios de voz. En este caso, el operador no limita la conectividad entre los distintos activos cibernéticos.
4.	Infraestructura APN privada que aplica un aislamiento lógico entre los activos cibernéticos	El activo cibernético está conectado a una red de comunicación que, según decida la organización, permite la conectividad a servicios de datos públicos (como Internet) y/o servicios de voz. En este caso, el operador limita la conectividad entre los distintos activos cibernéticos.

Por su parte, en el cuadro 3 se muestra una visión de conjunto de los tipos de tecnología SIM.

Cuadro 3. Tipos de tecnología SIM

	Nombre de la tecnología	Descripción
1.	SIM	Esta tecnología se basa en el uso de una tarjeta electrónica física, que permite la itinerancia (*roaming*) entre un activo cibernético y otro cuando su identidad de graba a nivel de *software*. La tarjeta está adaptada para trabajar con un único proveedor celular (perfil de trabajo único).
2.	eSIM	Esta tecnología se basa en el uso de una tarjeta electrónica física que forma parte integral del activo cibernético. La tarjeta está adaptada para trabajar con varios proveedores celulares diferentes (perfil de trabajo múltiple) y puede ser programada de forma remota y/o mediante una aplicación del proveedor celular instalada en el activo cibernético y/o mediante un código de respuesta rápida (QR, por sus siglas en inglés). En la actualidad, el uso de eSIM es más amplio en soluciones del tipo Internet de las cosas (IoT, por sus siglas en inglés).
3.	SIM virtual	La base de esta tecnología es el uso de una "tarjeta basada en *software*", que está adaptada para trabajar con varios proveedores celulares diferentes (perfil de trabajo múltiple) y puede ser programada de forma remota y/o mediante una aplicación del proveedor celular instalada en el activo cibernético y/o mediante un código QR.

Por razones de comodidad, en el documento se utiliza el término "SIM" como nombre general para las distintas tecnologías de trabajo. Donde sea necesario hacer énfasis en una tecnología específica, se indicará el nombre de esa tecnología explícitamente.

Las organizaciones que estén interesadas en utilizar una infraestructura APN privada deben, en primer lugar, celebrar un acuerdo contractual con un proveedor celular que ofrezca ese servicio, teniendo en cuenta que el suministro de capacidades de seguridad puede variar considerablemente entre un proveedor y otro.

Por ejemplo, el método de autenticación de activos cibernéticos puede basarse en la identidad IMSI asignada a una tarjeta SIM específica, un certificado digital instalado en el activo cibernético, un nombre de usuario y contraseña almacenados en el activo cibernético, el número de identificación único del dispositivo (como la identidad internacional de equipo móvil [IMEI, por sus siglas en inglés]) o una combinación de varios métodos de autenticación. Otro ejemplo son los casos en los que un proveedor celular permite a la organización realizar una autenticación independiente de los activos cibernéticos en su poder, dirigiendo al servidor RADIUS de la organización o bien de otra manera. Como último ejemplo, cabe destacar que el método de gestión de los activos cibernéticos autorizados para conectarse a la infraestructura APN privada también puede diferir entre distintos proveedores móviles, ya que algunos permiten al cliente que lleve a cabo una gestión independiente a través de una interfaz de Internet, mientras que otros requieren ponerse en contacto con el centro de servicio o la persona de contacto que trabaje con la organización de forma regular.

Además de las ventajas de seguridad inherentes al uso de una infraestructura APN privada, esta configuración de trabajo no brinda un alto nivel de seguridad, por lo que es necesario implementar controles complementarios adecuados.

/01. Finalidad y objetivos

Esta publicación presenta recomendaciones de implementación para la seguridad de infraestructuras APN privadas.

/02. Grupo destinatario

Esta publicación ha sido elaborada para Directores de Seguridad de la Información (CISO, por sus siglas en inglés), profesionales de metodología de ciberseguridad, profesionales de implementación de ciberseguridad y profesionales de tecnologías de ciberseguridad (arquitectos de ciberseguridad), así como personal de comunicación de datos, informática, tecnologías de la información (TI) y sistemas.

Otras partes que pueden beneficiarse con esta publicación son el Gerente de Sistemas de Información (CIO, por sus siglas en inglés), el Gerente de Privacidad de Datos (DPO, por sus siglas en inglés) y las entidades comerciales que deban aprobar la evaluación de riesgos del activo cibernético o del proceso comercial.

/03. Alcance de la publicación

Esta publicación es una herramienta para mejorar el nivel de seguridad de la APN privada utilizada por la organización mediante la aplicación de controles de protección adecuados.

Sin embargo, no busca reemplazar las instrucciones del fabricante ni incluye una ampliación relativa a temas sobre los que la Dirección Nacional de Ciberseguridad de Israel (INCD, por sus siglas en inglés) haya elaborado y publicado documentos específicos. Un ejemplo de esos temas es la protección de la red de tecnología de la información y las comunicaciones (TIC), respecto de la cual es posible obtener respuestas en el marco de la ***Metodología de Ciberdefensa para Organizaciones 1.0***, redactada y publicada por la INCD.[7]

Por otra parte, esta publicación no incluye cómo abordar las capacidades de un atacante en el campo de la inteligencia de señales (SIGINT, por sus siglas en inglés).

7. El documento se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad.**

/04.
Amenazas derivadas del uso de una infraestructura APN privada

El cuadro 4 describe las principales amenazas derivadas del uso de una infraestructura APN privada.

Cuadro 4. Principales amenazas contra una infraestructura APN

	Nombre de la amenaza	Descripción
1.	Ilusión de seguridad	Muchas organizaciones consideran una infraestructura APN como una solución con un alto nivel de seguridad, pese a que la realidad muestra que este no es el caso.
2.	Interceptación (*eavesdropping*)	La infraestructura celular hace uso de una variedad de tecnologías (manteniendo la compatibilidad con versiones anteriores). Con algunas de ellas, transmite la información de manera visible (texto claro) y utiliza protocolos de seguridad débiles. Como resultado de ello, existen casos en los que un atacante puede interceptar una llamada/información transmitida por un medio celular. El método de interceptación más simple se basa en la explotación de vulnerabilidades integradas en la infraestructura 1G/2G o en aquellos casos en los que es posible "bajar" los protocolos de comunicación a una versión anterior. Sin embargo, los atacantes que cuenten con los medios y las capacidades necesarias podrán realizar acciones similares con una infraestructura 4G/5G.
3.	Exposición de información sobre la identidad y las características técnicas del activo cibernético	Es habitual ver que los protocolos celulares son compatibles de forma predeterminada con la transmisión visible de información sobre la identidad y características técnicas del activo cibernético (como el tipo de sistema operativo y su versión). La obtención de información de este tipo por parte de un atacante puede facilitarle significativamente la realización de un plan de ataque (por ejemplo, aprovechando una vulnerabilidad conocida en el sistema operativo).
4.	Ataque de intermediario (MITM, por sus siglas en inglés) o inyección de contenido malicioso	La infraestructura celular hace uso de una variedad de tecnologías (manteniendo la compatibilidad con versiones anteriores). Con algunas de ellas, transmite la información de manera visible como texto claro y/o utiliza protocolos de seguridad débiles (como el protocolo del sistema de señalización No. 7 [SS7]). Debido a ello, un atacante podría materializar un ataque MITM para recopilar información sensible/confidencial, acosando al usuario, inyectando contenido malicioso (como *software* malicioso [*malware*]) o dirigiendo el tráfico de usuarios legítimos hacia el atacante mediante la suplantación (*spoofing*) del sistema de nombres de dominios (DNS, por sus siglas en inglés),[8] etcétera.

8. Esto es conocido como un ataque aLTEr. Véase **https://montsecure.com/research/alter-attack/.**

	Nombre de la amenaza	Descripción
5.	Robo de identidad (*spoofing*)	La infraestructura celular hace uso de una variedad de tecnologías (manteniendo la compatibilidad con versiones anteriores). Con algunas de ellas, transmite la información de manera visible como texto claro y/o utiliza protocolos de seguridad débiles. A causa de esto, un atacante con acceso a la red celular puede robar una identidad IMSI legítima (como en un ataque ToRPEDO, en el que el atacante envía comandos al activo cibernético mediante paginación sin que este tenga conocimiento de ello; un ataque PIERCER, en el que el atacante detecta e identifica el IMSI del activo cibernético directamente; o un craqueo de IMSI [*IMSI-cracking*] en el que el atacante "adivina" qué IMSI fue utilizada),[9] con lo que obtiene acceso a la infraestructura APN privada. Para ocultar sus actividades, el atacante puede llevar a cabo un ataque de denegación de servicio (DoS, por sus siglas en inglés) contra el activo cibernético legítimo, evitando al mismo tiempo que se emita una advertencia por intentos de conexión. Cabe destacar que el costo de una herramienta de ataque del tipo IMSI Catcher es de unos pocos miles de dólares y puede adquirirse libremente por Internet, y que en la actualidad estas herramientas pueden operarse sin necesidad de un alto nivel de conocimientos.
6.	Asignación IMSI/SIM no autorizada por un error humano	Es habitual que para añadir un nuevo activo cibernético a la infraestructura APN privada se requiera introducir manualmente el código IMSI/SIM, con lo que un error humano puede permitir un acceso no autorizado.
7.	Asignación IMSI/SIM no autorizada de manera deliberada	Una parte interna en el proveedor celular u otra parte que haya tomado el control de una infraestructura celular (incluyendo interfaces de gestión externas) puede vincular una IMSI/SIM maliciosa propia a la infraestructura APN privada como paso previo para lanzar un ataque contra la organización.
8.	No eliminación de la asignación IMSI/SIM del registro en la infraestructura APN privada	Es frecuente que las organizaciones tengan dificultades a la hora de eliminar de manera inmediata un registro IMSI/SIM que se haya perdido, haya sido robado o que ya no sea necesario para el trabajo continuo en la infraestructura APN privada. Esto permite que una parte con acceso a IMSI/SIM obtenga conectividad a la organización.
9.	Eliminación de IMSI/SIM registradas y/o borrado de la APN o ataque DoS	Una parte interna en el proveedor celular u otra parte que haya tomado el control de una infraestructura celular (incluyendo interfaces de gestión externas) puede eliminar IMSI/SIM registradas y/o borrar los ajustes de configuración de la infraestructura APN privada, realizando así un ataque DoS transversal.
10.	Existencia de conectividad no deseada a Internet	Debido a un error de configuración o una acción maliciosa, la infraestructura APN puede proporcionar conectividad a Internet a los activos cibernéticos, con lo que incrementa la superficie de ataque y permite una filtración de información por este canal.
11.	Duplicado físico de la tarjeta SIM y similares	Un usuario que entregue el activo cibernético para su reparación en un laboratorio externo, en un control fronterizo o en otro lugar, podría estar permitiendo que estas partes realicen un duplicado de la tarjeta SIM y similares, con lo que pueden obtener conectividad a la infraestructura APN privada.
12.	Ataque de intercambio de SIM (*SIM swapping*, también conocido como *SIM porting*, *port out fraud*, *phone porting* y *SIM hijacking*)	Se dan casos en los que un atacante puede realizar una itinerancia (*roaming*) en una SIM legítima para que esté registrada a su nombre, con lo que obtiene acceso a la infraestructura APN privada. Alternativamente, incluso si no tiene éxito en la primera fase, el atacante podría utilizar los datos legítimos introducidos en la fase preliminar para "persuadir" al equipo de soporte del operador para que realice el registro en la infraestructura APN privada.

9. Para más información, véase ***Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information*** (en inglés) disponible en: **https://cdn.comparitech.com/wp-content/uploads/2024/02/LTE-torpedo-NDSS19.pdf.**

	Nombre de la amenaza	Descripción
13.	Introducción de un *malware*	El uso de una infraestructura APN privada no garantiza resistir a la introducción de un *malware* en la red de la organización. Además, si no se configura una separación suficiente entre los activos cibernéticos vinculados a la infraestructura APN privada, ello podría permitir que se introduzca un *malware* entre los diferentes activos cibernéticos.
14.	Fuga de información de la base de datos	La base de datos del proveedor celular podría incluir detalles ocultos, como la identidad de los usuarios, la estructura organizacional, la distribución geográfica de los activos cibernéticos (incluyendo su ubicación física en tiempo real) dirección IP, etc. A la vista de esto, la filtración de este tipo de información (ya sea debido a las acciones de una amenaza interna o por algún otro motivo) podría ser una oportunidad perfecta para recopilar inteligencia para operaciones.
15.	Infiltración de un *malware* en el activo cibernético mediante el envío de SMS o mensajería multimedia (MMS, por sus siglas en inglés)	Existen casos en los que es posible infiltrar un *malware* en el activo cibernético mediante el envío de SMS/MMS, incluso sin necesidad de que el usuario lleve a cabo una acción activamente.
16.	Conversión del activo cibernético en un portal puente (*bridge portal*)	La existencia de una interfaz inalámbrica en el activo cibernético puede convertirlo en un portal puente entre redes, sin que la organización tenga conocimiento de ello. Esto puede permitir que un atacante obtenga acceso a la red de la organización utilizando el medio inalámbrico.

	Nombre de la amenaza	Descripción
17.	Ataque contra el representante de la organización responsable de la operación	Un atacante podría llevar a cabo un ataque previo contra el representante de la organización responsable de operar la infraestructura APN privada (como un ataque de suplantación de identidad [*phishing*]), a fin de utilizar la información de dicho representante para convencer al proveedor celular de que le permita obtener conectividad a la infraestructura APN privada.
18.	Uso indebido de una eSIM o una SIM virtual	Una eSIM permite programar una tarjeta física integrada mediante una aplicación instalada en el activo cibernético al conectarla de forma remota o mediante un código QR. Una SIM virtual se basa únicamente en *software* y es la tecnología más reciente en la actualidad. La transición a una infraestructura que permita la programación incrementa considerablemente la superficie de ataque (en particular la SIM virtual), lo que puede facilitar la realización de acciones maliciosas por parte de un atacante.
19.	Ataque de drenaje de la batería (*battery draining attack*)	Un conjunto de ataques DoS cuyo objetivo es acortar la vida útil de la batería de un activo cibernético. Un ejemplo habitual es llevar a cabo un gran número de consultas innecesarias al activo cibernético para hacer que no entre en modo de suspensión (ahorro de energía), o para alterar la actividad de la red celular y obligar así al activo cibernético a iniciar consultar repetidas a la BTS.
20.	Desconexión del activo cibernético de la red celular (*signaling DoS*)	Un caso particular de materialización de un ataque DoS, en el que el atacante envía solicitudes repetidas para crear una llamada con el activo cibernético y a continuación abandona la llamada. El proveedor celular puede detectar e identificar este comportamiento inusual y tomar acciones al respecto de manera proactiva, como desconectar el activo cibernético de la red celular.
21.	Daños al desempeño celular (ataque *bidding-down*)	Un caso particular de materialización de un ataque de DoS, en el que el atacante hace que el activo cibernético utilice una tecnología celular más antigua (como 2G), lo que ocasiona una tasa de tráfico más baja.

	Nombre de la amenaza	Descripción
22.	Localización de SIGINT	El uso de señales electrónicas para localizar físicamente el activo cibernético, incluyendo la cantidad de activos operados en un área determinada. Además, existen métodos de ataque avanzados que permiten expandir esta capacidad de modo que el atacante sea capaz de producir información sobre el área de trabajo física y el orden de fuerzas existente en dicha área, aun cuando la actividad celular no sea alta en ella.
23.	Ocultamiento de la existencia de una transmisión celular maliciosa	La cobertura de las redes celulares es extensa y también cubre áreas de trabajo sensibles/críticas. Además, es habitual que los usuarios utilicen un teléfono celular con frecuencia durante el trabajo. A la vista de esto, en ocasiones es difícil distinguir entre una radiotransmisión legítima y una maliciosa. Así, por ejemplo, la transmisión de un módem celular malicioso (*rouge hardware*) que esté conectado a un activo cibernético (para vincularlo a un servidor de mando y control [C&C, por sus siglas en inglés]) puede implementarse como parte de transmisiones legítimas en el área de trabajo, y localizar dicha transmisión no es algo trivial para muchas organizaciones.
24.	Modulación maliciosa en un canal celular legítimo	El uso extenso de una infraestructura celular permite a atacantes potenciales modular información en un canal celular legítimo. Por lo general, los equipos de ciberseguridad tienen grandes dificultades a la hora de detectar e identificar este tipo de actividad.
25.	Instalación de un *malware* oculto en los activos cibernéticos del proveedor celular	Los proveedores celulares llevan a cabo adquisiciones de activos cibernéticos a distintos proveedores del extranjero, algunos de los cuales pueden estar bajo control externo. Debido a ello, estos proveedores pueden instalar en los activos cibernéticos *malware* oculto que podrían desplegar en un día crucial.

En aras de la simplicidad, se utiliza el teléfono móvil como ejemplo de activo cibernético al que se aplican las amenazas. Sin embargo, debe tenerse en cuenta que las amenazas también son relevantes para otros activos cibernéticos, como las computadores portátiles o unidad terminal remota/controlador lógico programable (RTU/PLC, por sus siglas en inglés) con un módulo celular integrado. Debido a ello, pueden existir situaciones en las que un activo cibernético esté conectado a la red celular durante mucho tiempo sin una supervisión cercana por parte de personas.

/05.

Recomendaciones para la seguridad de infraestructuras APN privadas

Esta sección presenta una lista de recomendaciones de implementación, cuya correcta aplicación contribuirá a la seguridad de la infraestructura APN privada.

Cuadro 5. Recomendaciones para la seguridad de infraestructuras APN

N.°	Recomendación	Estado (realizada/ no realizada)
Recomendaciones generales		
1.	Se recomienda realizar una evaluación de riesgos (*risk assessment*). Como parte de las actividades, se aconseja asegurarse de que la mesa directiva sea consciente de que el uso de una infraestructura APN privada no brinda un alto nivel de seguridad.	
2.	Se recomienda mapear las interfaces de configuración de la infraestructura APN privada, haciendo referencia al ciclo de vida (como adición, sustracción, etc.). Debe prestarse atención a la existencia de interfaces de gestión externas, como sitios web y la interfaz de programación de aplicaciones (API, por sus siglas en inglés).	
3.	Se aconseja utilizar una infraestructura APN privada que aplique un aislamiento lógico entre activos cibernéticos, bloquee el acceso a Internet e impida la posibilidad de utilizar el canal de voz y las funcionalidades relacionadas, como SMS y MMS.	
4.	Se sugiere realizar una separación entre IMSI/SIM que sean utilizadas para necesidades privadas y para los fines del trabajo.	
5.	Se recomienda configurar a la organización o la parte correspondiente como un operador de red virtual móvil (MVNO, por sus siglas en inglés) a fin de dificultar las actividades del atacante. Por ejemplo, es posible cambiar de manera aleatoria las identidades de la SIM (al azar o proactivamente), además de ocultar una ubicación o facilitar una ubicación errónea. Sin embargo, deben tenerse en cuenta las entradas (*inputs*) resultantes de esta configuración de trabajo.	
6.	Se aconseja asegurarse de que se utilice un nombre de APN que no revele la función de la infraestructura y/o el nombre de la organización.	
7.	Se sugiere realizar auditorías periódicas y sin previo aviso, y comprobar la exactitud del mapeo del IMSI/SIM en los sistemas del proveedor celular con respecto al mapeo más reciente del que disponga la organización.	

N.°	Recomendación	Estado (realizada/ no realizada)
Recomendaciones generales		
8.	Se recomienda utilizar elementos de autenticación adicionales al otorgar acceso a la infraestructura APN privada y no confiar únicamente en los elementos de autenticación IMSI/SIM. Los siguientes son los elementos de autenticación mínimos que se recomienda implementar: i. Un elemento de autenticación del tipo identificador de enumeración (como IMEI o un identificador de equipo móvil [MEID, por sus siglas en inglés]), a fin de realizar una correlación a la identificación SIM. Los que siguen son los elementos de identificación más avanzados que se recomienda implementar (además del mínimo indicado anteriormente): ii. Un elemento de autenticación del tipo certificado digital. iii. Un elemento de autenticación del tipo perfil de dispositivo (*device profiling*).	
9.	Se aconseja securizar los activos cibernéticos de modo que no utilicen tecnología/protocolos con deficiencias que puedan ser aprovechadas con una relativa facilidad, como 3G y versiones inferiores. Sin embargo, deben examinarse las consecuencias operativas, debido a que las redes 4G/5G aún no tienen una cobertura completa en todas las regiones.	
10.	Se sugiere securizar el activo cibernético aplicando los siguientes requisitos: i. Bloquear la capacidad del usuario para realizar modificaciones no autorizadas en el perfil de trabajo o en los ajustes de configuración de la infraestructura APN privada en el activo cibernético. ii. Bloquear la capacidad de habilitar la itinerancia (*roaming*) del activo cibernético a otro proveedor celular estableciendo una configuración de trabajo con un único proveedor celular.	

N.°	Recomendación	Estado (realizada/ no realizada)
Recomendaciones generales		
	iii. Desactivar las alertas de emergencia (difusión de celda [CB, por sus siglas en inglés]), debido a que éstas se transmiten por un canal de control (una especie de red fuera de banda [OOB, por sus siglas en inglés]) sin tener en cuenta la existencia de una infraestructura APN privada. Esto puede ponerse en práctica realizando una securización mediante un sistema de gestión de dispositivos móviles (MDM), o bien por otro medio.	
11.	Se recomienda asegurarse de que el activo cibernético utilice mecanismos aceptados para hacer frente a un ataque DoS, como aplicar un umbral para las acciones a realizar en un momento dado.	
12.	Se aconseja aplicar los principios aceptados del ámbito de negación y engaño (D&D, por sus siglas en inglés), a fin de reducir el nivel de exposición de información auténtica sobre el activo cibernético y las características técnicas de este.	
13.	Se sugiere realizar comprobaciones periódicas para detectar e identificar actividades de transmisión anormales, incluyendo la modulación maliciosa en un canal de transmisión legítimo.	
14.	Se recomienda priorizar el uso de un módem celular (por ejemplo, un *Netstick*) que no sea un enrutador, como alternativa al uso de teléfonos inteligentes, los cuales suelen ser más vulnerables.	
15.	Se aconseja implementar actualizaciones de seguridad (parches) con la frecuencia recomendada por el fabricante de los activos cibernéticos involucrados en cada proceso. Esto incluye asegurarse de que se apliquen actualizaciones en los activos cibernéticos gestionados por el proveedor móvil.	

N.°	Recomendación	Estado (realizada/ no realizada)
Seguridad de la conectividad a la red de la organización		
16.	Se sugiere asegurarse de que la conectividad a la organización desde la infraestructura APN se lleve a cabo mediante el uso de una zona desmilitarizada (DMZ, por sus siglas en inglés) específica (que no esté conectada a Internet) que comprenda el uso de medidas de seguridad aceptadas. Los siguientes son ejemplos de implementación: i. Filtro de tráfico – cortafuegos. ii. Filtro de contenido – cortafuegos de lenguaje de marcado extensible (XML, por sus siglas en inglés) o cortafuegos de aplicaciones web (WAF, por sus siglas en inglés).	
17.	Se recomienda utilizar tecnología de red privada virtual/ perímetro definido por *software* (VPN/SDP, por sus siglas en inglés) u otra tecnología diferente para vincular el activo cibernético a la red de la organización, adoptando principios aceptados[10] tales como: i. Aplicación de cifrado de extremo a extremo (E2EE, por sus siglas en inglés), con independencia de la infraestructura APN privada. ii. Uso de un elemento de autenticación único adicional para autenticar el activo cibernético antes de otorgar acceso a la red interna de la organización. iii. Autenticación mutua de las partes en una conversación (seguridad de la capa de transporte mutua [mTLS, por sus siglas en inglés]). iv. Autenticación adaptativa (*adaptive authentication*). v. Autenticación continua (*continuous authentication*).	

10. Para ampliar este tema, véase el documento ***Autenticación multifactor avanzada ante amenazas de ciberseguridad*** de próxima publicación dentro de esta serie de guías de buenas prácticas en ciberseguridad.

N.°	Recomendación	Estado (realizada/ no realizada)
Seguridad de la conectividad a la red de la organización		
	vi. Inspección continua del nivel de higiene tecnológica (*hygiene technology*) del activo cibernético. vii. Prevención de la capacidad de recuperar información histórica (*replay-resistance*). viii. Comprobación de que las claves secretas a largo plazo que se utilizan para compartir claves de llamada no supongan un peligro para la confidencialidad de las claves de llamada creadas por el protocolo en el pasado. Un ejemplo de implementación es la aplicación de principios *Perfect Forward Secrecy* (PFS) aceptados. ix. Existencia de una actividad (*session*) única del activo cibernético en la infraestructura APN.	
Hacer frente a incidentes anormales		
18.	Se aconseja asegurarse de que el procedimiento de respuesta a incidentes cibernéticos incluya una referencia a la forma de hacer frente a incidentes en el proveedor celular que puedan afectar a la seguridad de la infraestructura APN privada.	
19.	Se sugiere asegurarse de que la organización realice prácticas periódicas sobre cómo hacer frente a escenarios de ataque relevantes para las infraestructuras APN privadas.	
Cadena de suministro		
20.	Se recomienda establecer jurídicamente unos procesos de trabajo regulados con el proveedor celular, en los que se haga referencia a los escenarios de ataques y las maneras de actuar frente a ellos.	
21.	Se aconseja asegurarse de que se utilicen aplicaciones o implementaciones de una fuente de confianza. Debe tenerse en cuenta que el uso de una infraestructura APN no proporciona una respuesta a esta amenaza.	

N.°	Recomendación	Estado (realizada/ no realizada)
Cadena de suministro		
22.	Se sugiere establecer jurídicamente con el proveedor celular los niveles de servicio que se esperan de la infraestructura APN privada, en los que se haga referencia a escenarios comunes, como la recepción de prioridad con respecto a otros clientes en caso de producirse una emergencia o una carga anormal.	
23.	Se aconseja llevar a cabo de forma independiente verificaciones de antecedentes de los empleados de los proveedores que tengan acceso para gestionar/recibir información sobre la infraestructura APN privada.	
24.	Se sugiere realizar auditorías periódicas del proveedor en relación con la gestión de la APN.	
25	Se recomienda asegurarse de que los proveedores de servicios pertinentes cumplan con los requisitos para la cadena de suministros[11] de la INCD.	

11. El cuestionario para proveedores para reforzar la cadena de suministro se encuentra incluido en el documento ***Cadena de suministro***, el cual forma parte de esta serie de guías de buenas prácticas en ciberseguridad y disponible a través del siguiente enlace: **https://publications.iadb.org/es/cadena-de-suministro-cuando-todos-los-eslabones-son-fuertes-su-organizacion-esta-protegida-mejores.**

Anexos

Estos anexos brindan información al lector sobre el desarrollo del documento, las partes que han intervenido en el proceso de elaboración y el envío de reacciones y comentarios sobre el contenido, para una mayor transparencia y una adecuada divulgación del proceso y las diferentes partes involucradas.

Anexo 1. Proceso de trabajo para la redacción de esta publicación

Cómo se ha elaborado el documento: estudio de mercado, temario, comparación a nivel mundial

01

Estudio de documentación y estandarización a nivel mundial, como el Instituto Nacional de Estandarización y Tecnología (NIST, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés). (los principales ejemplos se muestran en el **anexo 2: Documentos aplicables**).

02

Estudio de publicaciones aceptadas en este ámbito (los principales ejemplos se muestran en el **anexo 2: Documentos aplicables**).

03

Recepción de observaciones y comentarios de la compañía FirstPoint Mobile Guard Ltd.

Anexo 2. Documentos aplicables

Esta sección contiene las fuentes de información utilizadas a la hora de elaborar este documento.

Fuentes de información en español

Dirección Nacional de Ciberseguridad de Israel (incluidos dentro de esta serie de guías de buenas prácticas en ciberseguridad)

- Cuestionario de proveedores para reforzar la cadena de suministro. Disponible en: **http://www.iadb.org/document.cfm?id=EZSHARE-37811622-6.**
- Endurecimiento de sistemas informáticos (de próxima publicación).
- Metodología de ciberdefensa para organizaciones 1.0. Disponible en: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad.**
- Preparación organizacional para una crisis cibernética. Disponible en: **https://publications.iadb.org/es/preparacion-organizacional-para-una-crisis-cibernetica-caracterizacion-y-requisitos-de-los-equipos.**
- Uso de servicios en la nube: adenda a la metodología de ciberdefensa para organizaciones. Disponible en: **https://publications.iadb.org/es/uso-de-servicios-en-la-nube-adenda-la-metodologia-de-ciberdefensa-para-organizaciones-mejores.**

Fuentes de información en hebreo

Dirección Nacional de Ciberseguridad de Israel

- Fortalecimiento de la identificación de usuarios en los sistemas e infraestructuras de la organización mediante el uso de autenticación multifactor. Disponible en: **https://www.gov.il/he/pages/mfa.**

- Tendencia al alza en ataques que utilizan SIM SWAPPING. Disponible en: **https://www.gov.il/he/pages/sim-swapping.**

General

- Acerca de GSM, VoIP y números ocultos. Disponible en: **https://www.digitalwhisper.co.il/files/Zines/0x1E/DW30-3-GSMVOIP.pdf.**

Fuentes de información en inglés

General

- 5G Speed Is Data Transmission in Real Time. Disponible en: **https://www.telekom.com/en/company/details/5g-speed-is-data-transmission-almost-in-real-time-544498.**
- aLTEr Attack. Disponible en: **https://montsecure.com/research/alter-attack/.**
- APN Settings. Disponible en: **https://www.apnsettings.org/.**
- Breaking LTE on Layer Two. Disponible en: **https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2023/10/0008-breaking_lte_on_layer_two.pdf.**
- On Cellular Encryption. Disponible en: **https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/.**
- IMSI Generator. Disponible en: **https://www.imei.info/imsi/.**
- New Vulnerabilities in 5G Networks. Disponible en: **https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf.**
- Overview of Cellular Mobile Network Standards. Disponible en: **https://www.1nce.com/en-us/resources/news/blog/cellular-mobile-standards.**

- Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. Disponible en: **https://cdn.comparitech.com/wp-content/uploads/2024/02/LTE-torpedo-NDSS19.pdf.**
- A Step by Step Guide to SS7 Attacks. Disponible en: **https://web.archive.org/web/20250429183029/https://firstpoint-mg.com/blog/ss7-attack-guide/.**

Instituto Nacional de Estandarización y Tecnología (NIST)

- Guidance for Improving LTE-based Mobile Communications Security. Disponible en: **https://www.nist.gov/publications/guidance-improving-lte-based-mobile-communications-security.**
- Guidelines for Managing the Security of Mobile Devices in the Enterprise, Rev. 2 (Borrador). Disponible en: **https://csrc.nist.gov/pubs/sp/800/124/r2/ipd.**
- Guide to LTE Security. Disponible en: **https://www.nist.gov/publications/guide-lte-security.**

Nombre del punto de acceso, del inglés *Access Point Name* (APN), es un término colectivo para un grupo de configuraciones de trabajo aceptadas cuya finalidad es permitir que el proveedor de telefonía celular (u otra parte autorizada) supervise y controle la actividad de un activo cibernético (como un teléfono móvil) vinculado a la infraestructura de la red celular.

En este aspecto, a nivel de ciberseguridad, las organizaciones que utilicen una red celular pueden reducir la superficie de ataque mediante el uso de una infraestructura APN privada, la cual puede brindar servicios de valor añadido como el uso de números acortados entre usuarios de esta. Además los activos cibernéticos que formen parte de la infraestructura APN privada pueden recibir un nivel de servicio más alto en caso de producirse una sobrecarga o un incidente de emergencia que afecte a la infraestructura celular.

Esta publicación presenta recomendaciones de implementación para la seguridad de infraestructuras APN privadas, lo que constituye una herramienta para mejorar el nivel de seguridad de la organización mediante la aplicación de controles de protección adecuados. La publicación ha sido elaborada para Directores de Seguridad de la Información, profesionales de metodología de ciberseguridad, profesionales de implementación de ciberseguridad y profesionales de tecnologías de ciberseguridad (arquitectos de ciberseguridad), así como personal de comunicación de datos, informática, tecnologías de la información y sistemas. Otras partes que también pueden beneficiarse con esta publicación son el Gerente de Sistemas de Información, el Gerente de Privacidad de Datos y las entidades comerciales que deban aprobar la evaluación de riesgos del activo cibernético o del proceso comercial.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación
- **B.22** Protección de los servicios de nube pública ante amenazas de *ransomware*

Volumen C: Desarrollo seguro de *software*