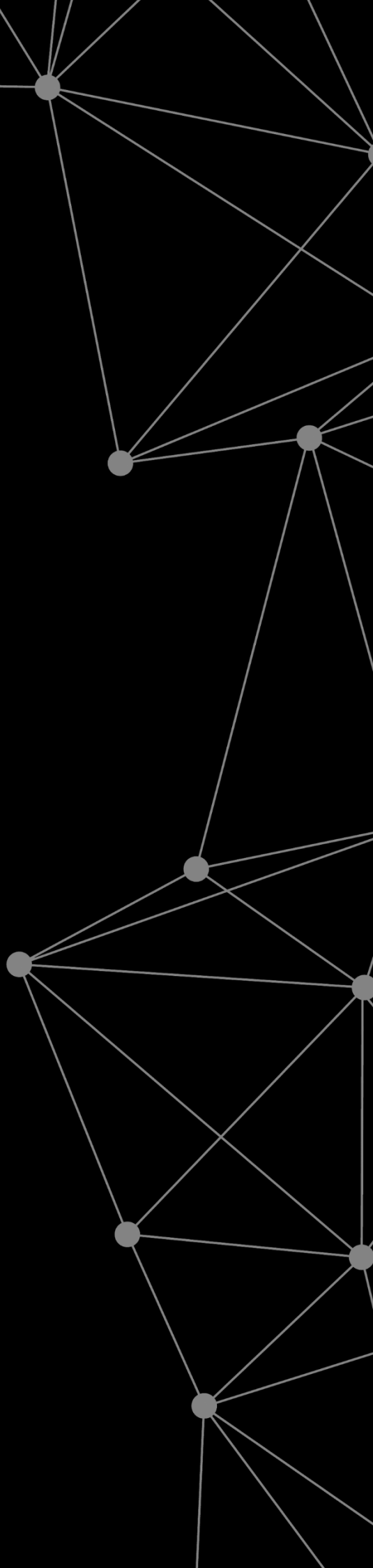
Guía para Iniciados en Ciberseguridad

Un puñado de consejos para estar bien preparado



Juan Montalvo Fernández

Contenido

Misión

El objetivo de esta guía es ayudarte en tus inicios en el mundo de la Ciberseguridad. No se trata de un documento técnico. No voy a enseñarte a configurar Kali, ni a hackear, ni a montarte un laboratorio con máquinas virtuales. Voy a contarte qué puedes encontrarte cuando empieces a trabajar en Ciberseguridad y a darte algunos trucos y consejos para que el camino te sea algo más fácil.

Esta guía va a ser mejor aprovechada por perfiles junior que están comenzando y por personas que han decidido dar un giro a su carrera profesional para adentrarse en esta práctica tan demandada, pero también puede venir bien para refrescar la mente e incluso dar alguna idea a los que llevan más tiempo.

Introducción

Vivimos una burbuja. La enésima de los últimos años. La burbuja tecnológica ha llegado para quedarse durante mucho tiempo, ya que el mundo se ha vuelto completamente tecnológico, y no piensa dejarlo. Dentro de todas las áreas, me atrevería a decir que, Ciberseguridad junto a DevOps son las que mayor demanda de profesionales tienen.

Es un momento dulce, recibes decenas de ofertas a la semana, algunas irrisorias en cuanto a condiciones, y otras que te hacen pensar hasta dónde podría llegar tu salario. Pero este escenario también está atrayendo a muchos pseudo-profesionales y personas recicladas de otros puestos, que están abordando tareas para las cuáles no están cualificados. No lo llamaría intrusismo, pero sí desesperación por parte de las empresas e imprudencia por parte de los trabajadores.

Odio las frases de importantes “filósofos” y gurús de su campo, pero hay una que se atribuye a Warren Buffet que me parece afilada y certera como una flecha: *“Sólo cuando baja la marea se ve quién nadaba desnudo”*. ¿Qué quiero decir con esto? Que llegará un punto en el que la burbuja estalle, o al menos se haga más pequeña, y se descubra quién no es un verdadero profesional. Muy probablemente esto supondrá sorpresas y despidos por igual.

Por este motivo, te aconsejo, casi te obligo a que te formes, te actualices, practiques y nunca dejes de aprender y de ser curioso. Porque esos son los principales motores de una carrera profesional de valor.

Me he basado en mis años de experiencia para contar todo lo que cuento, todo es real, y creo que va a serte útil para el día a día.

Con suerte, este será el primero de varios volúmenes.

Un Poco Sobre Mí

No quiero aburrirte con mi experiencia en el sector. Parar resumir, soy un Ingeniero de Seguridad, que lleva trabajando más de 11 años en este campo y lo ha visto cambiar y evolucionar.

Desde la Seguridad perimetral y las arquitecturas 100% on-premise hasta las actuales cloud, he aprendido cómo proteger diferentes tipos de infraestructuras de una forma eficiente.

Este es mi perfil en LinkedIn: https://www.linkedin.com/in/juan-montalvo-23a37144/

1. Conoce el Sector

El sector financiero no sufre las mismas amenazas que, por ejemplo, el sector de la alimentación, o la industria petrolera. En unos quieren robar datos, en otros desviar dinero, en otros tirar infraestructuras críticas… Cada tipo de empresa y su idiosincrasia conllevan cierto tipo de amenazas. Algunas de ellas pueden coincidir, por qué no, pero muchos casos de uso serán diferentes. Por esto te recomiendo analizar bien el sector al que has ido o vas a ir a parar. Esta tarea de reconocimiento pasa por investigar qué tipo de ataques han sufrido las empresas del sector en el pasado, las amenazas a las que se ven expuestas, un histórico de vulnerabilidades y otros detalles. Te será muy útil conocer los sistemas más implementados para tener un listado de vulnerabilidades y saber por dónde empezar a remediar desde el primer día.

Este tipo de análisis no debería llevarte más de 2 o 3 días, al fin y al cabo se trata de leer mucho. No te centres exclusivamente en empresas españolas, ve más allá, porque las ciber amenazas son globales.

Con este análisis en tu mano, es muy probable que tu eficiencia se dispare, ya que vas a conocer de antemano el escenario global en el que se encuentra tu compañía, y esto te va a permitir ser productivo desde una fase muy temprana.

2. Conoce la Arquitectura

Este trabajo no podrás llevarlo a cabo previo a la entrada a tu compañía (o sí, depende de las mañanas que te des con el hacking de caja negra :P). Se trata principalmente de conocer cómo está montada la infraestructura. Esta puede estar 100% on-premise (datacenters físicos), 100% cloud o puedes encontrarte un modelo híbrido, que creo es el más común.

De nuevo, cada modelo tiene una forma diferente de funcionar, y existen formas diferentes de protegerlos. Para serte sincero, lo más sencillo es un modelo 100% on-prem, ya que la visibilidad que aporta y la facilidad de acceso no se puede encontrar en la nube, pero este modelo lo conocemos los más viejos y, como nosotros o el diésel, tienen a desaparecer. Por lo tanto vamos a centrarnos en un entorno 100% cloud, ya que, en el medio plazo va a ser lo más extendido. Las empresas que no son ya 100% cloud están en un proceso de transformación digital para llevar sus recursos a AWS, GCP o Azure entre otras.

Proteger activos en la nube es, cuanto menos, abstracto. No puedes tocar y tienes que fiarte de diagramas de arquitectura que estarán desactualizados y obsoletos para saber qué tienes que securizar. En estos casos yo siempre sigo un férreo plan para poder empezar a trabajar sin perder la cabeza:

1. **Un inventario de activos**: Ya sean on-prem o cloud. Todo lo que pueda considerarse recurso es susceptible de ser atacado y, por lo tanto, tiene que ser protegido. Y mucho cuidado con el famoso “Shadow IT” porque puede convertirse en una pesadilla. Hay infinidad de buenas herramientas para hacer esto, unas open source, otras de pago, y también puedes hacerlo de manera manual, aunque como te imaginarás, tardarás bastante más tiempo.
2. **Una matriz de riesgos:** Cuando tengas esos activos, busca qué riesgos pueden correr, qué vulnerabilidades les aplican, y traza ciertos controles para mitigarlos. De ese modo habrás avisado de la situación y tendrás argumentos para trazar un plan.
3. **Acción:** Comienza a aplicar los controles y a proteger activos. Y no te olvides de mejorar las medidas de seguridad que ya estén implementadas.

Estos 3 pasos son imprescindibles dentro de cualquier sector, empresa o arquitectura. No importa de qué tipo sean.

3. Conoce las Herramientas

Con el paso del tiempo te darás cuenta de que hay infinidad de herramientas, infinidad de fabricantes e infinidad de posibilidades.

De hecho, muchas veces verás que diferentes herramientas de seguridad se pisan en algunas funciones, por lo que no será sencillo elegir, especialmente si te encuentras un campo baldío sin seguridad de ningún tipo.

Es muy importante que te quedes con lo más básico y sepas diferenciar un EDR de un XDR y un NDR, un IDS de un IPS, un WAF de un Firewall tradicional, un CASB de un CSPM y un SASE, un SIEM de un SOAR, etc… Al final verás que no es tan difícil y conocerás, al menos un par de productos para cada categoría.

Por si puedo hacerte la vida un poco más fácil, aquí van unos ejemplos:

- **EDR (Endpoint Detection and Response):** Crowdstrike, Checkpoint.
- **NDR (Network Detection and Response):** Darktrace, IBM Qradar.

- **XDR (Extended Detection and Response):** Palo Alto Cortex, Sophos Intercept X.
- **IDS (Intrusion Detection System):** Perimeter81, Snort.
- **IPS (Intrusion Detection System):** FireEye, Zscaler Cloud IPS.
- **WAF (Web Application Firewall):** Imperva, Akamai.
- **Firewall:** Fortinet, Checkpoint.
- **CASB (Cloud Access Security Broker):** Forcepoint, Proofpoint.
- **CSPM (Cloud Security Posture Manager):** Sysdig, Lacework.
- **SASE (Secure Access Service Edge):** Netskope, Palo Alto Prisma Access.
- **SIEM (Security Information and Event Management):** DataDog Security Monitoring, Splunk.
- **SOAR: (Security Orchestration, Automation, and Response):** Splunk Phantom, IBM Resilient.

Gartner no es la biblia

Pese a lo que te pueda parecer, sobre todo si comienzas en una consultora grande, Gartner no siempre tiene la razón. La mayoría de consultoras delega sus elecciones al Cuadrante Mágico de esta compañía, que es un referente sí, pero si hablas con los más experimentados, todos te dirán lo mismo: *"ahí aparecen los que más pagan"*. Y puede ser así, o no, yo no lo sé a ciencia cierta, pero lo que sí sé es que el Cuadrante Mágico puede servirte como guía, pero no te va ayudar a ceñirte al presupuesto, ni a cubrir los GAPs de seguridad que tenga tu empresa, ni a realizar el despliegue de la herramienta que elijas.

Por eso, siempre puedes echar un ojo al Cuadrante, pero te recomiendo que vayas más allá y consultes en foros especializados en Ciberseguridad. Además de esto, siempre puedes contactar con los fabricantes o distribuidores y solicitar una demo o una PoC (Proof of Concept) para probar las funcionalidades del producto en cuestión por ti mismo, normalmente en un laboratorio. De este modo, sacarás tus propias conclusiones, podrás otorgar una puntuación y saber si es el producto correcto o no.

Apuesta por el Open Source

A menudo se confunde el Open Source con productos muy básicos o incluso peligrosos y de muy mala calidad, pero lo cierto es que detrás de cada proyecto Open Source hay una comunidad importante de gente con mucho conocimiento y más voluntad que está continuamente aportando y actualizando dichos productos (véase Ubuntu por ejemplo). Estas herramientas pueden lograr un nivel de ajuste y personalización muy alto, por contra, suelen requerir bastante tiempo y recursos para su despliegue, ya que es un proceso que tendremos que realizar nosotros o con la ayuda de los equipos de despliegue encargados. En cualquier caso, recomiendo siempre buscar opciones Open Source a las

herramientas que tengas pensado implementar o incluso a las ya implementadas, ya que puedes llevarte una sorpresa en cuanto a las mejoras que pueden aportar y al dinero que puedes ahorrar a la empresa.

Los Estándares y Marcos de Seguridad

Los estándares y marcos de Seguridad te serán muy útiles para encontrar los GAPs de tu compañía y conocer las herramientas o mejores prácticas para atajarlos.

Estos estándares están desarrollados por equipos de profesionales del mundo de la Ciberseguridad, y son aplicables a los diferentes dominios que comprende.

Por enumerar algunos de los más importantes y que empieces a familiarizarte con ellos, tenemos NIST, OWASP, Mitre ATT&CK, ISO27001, PCI-DSS y CIS. Por supuesto existen más, dedicados a diferentes sectores y dominios dentro de la Ciberseguridad, ya irás conociéndolos con el tiempo y la experiencia.

Ten siempre a mano alguno de estos marcos de Seguridad, ya que son casi de obligada aplicabilidad para comenzar la base de la protección de una compañía.

4. ¡Alinéate con el Negocio!

¿Ves las exclamaciones? Están ahí por algo. Tanto si caes en un área técnica, como si caes en un área más enfocada a la gestión, tienes que llevar tatuada esta frase en tu memoria. Piensa una cosa, existe un departamento de Seguridad, porque previamente existía el Negocio, entonces, aplicar Seguridad afectando al Negocio sería absolutamente contraproducente. ¿Acaso quieres convertirte en una enfermedad autoinmune dentro de tu empresa? Lo dudo.

Déjame ahondar un poco más en este tema. Siempre que se realiza un plan de Seguridad, ya sea algo pequeño o un megaproyecto de varios meses y millones de euros, tiene que estar en línea con lo que se hace en la empresa y jamás interferir en las operaciones de la misma. Si despliegas y configuras un WAF para proteger tus activos en la nube, pero este bloquea el tráfico de las transacciones de tus clientes sería un desastre. Por este motivo debes aprender a convivir y a llevarte bien con las áreas que velan por el Negocio de la empresa: equipos financieros, de ventas, operaciones, desarrollo… Todos están ahí haciendo lo mismo que tú, su trabajo.

Siempre que se lleve a cabo cualquier iniciativa de Seguridad de cierta envergadura, es necesario consensuar con todos los interesados las tareas a

ejecutar para asegurarnos de que no vamos a causar una disrupción en el Negocio. El Negocio es lo que nos da de comer, y nosotros velamos porque esté seguro, es una relación de beneficio mutuo.

5. Los DevOps, ¡ay, los DevOps!

Hablo de DevOps porque llevo ya años caminando plácidamente por las nubes de AWS, Azure y otros, pero si estuviésemos hablando de entornos on-premise, el título sería “Los Sysadmin, ¡ay, los Sysadmin!”

Este grupito es muy interesante. Estamos hablando de perfiles críticos para la infraestructura, y también hablamos de bombas de relojería con accesos de administrador a todos los sistemas que te puedas imaginar. Son una parte crucial del Negocio, y como hemos dicho antes, no queremos interferir en el Negocio, así que lo único que nos queda es tenerlos monitorizados lo máximo posible para evitar un susto. Por lo general te encontrarás con gente que sabe lo que hace, pero no por ello tienen que tener conocimiento de Seguridad, por lo que es muy recomendable tener una relación estrecha con ellos. Una primera introducción y reuniones regulares serán suficientes para que haya una comunicación fluida.

Sé que parece de perogrullo, pero te recomiendo que tengas una muy buena relación con los equipos de DevOps, no porque sean “peligrosos” ya que se juegan mucho más que una bronca de Seguridad si hacen alguna trastada o cometen un error importante, sino porque te van a ayudar mucho a identificar activos, a entender la arquitectura de tu empresa y a realizar los despliegues de los productos de Seguridad que decidáis implementar.

6. Las Ramas de Ciber

Cuando comiences tu andadura en el fascinante y siempre cambiante mundo de la Ciberseguridad, te darás cuenta de que tienes un sinfín de caminos y posibilidades. Al principio te sentirás sobrepasado, pero verás que es cuestión de tiempo ubicarte en un lado u otro.

Te pondré algunos ejemplos para ir un poco más allá de la típica diferenciación entre perfil técnico o de gestión:

Analista de Seguridad / Consultor	Suele ser el comienzo habitual. Su función principal es el análisis y gestión de alertas y vulnerabilidades. Es una buena base para aprender a conocer herramientas y ver la gestión.
Ingeniero de Seguridad / Consultor	Otro comienzo, pero este con más recorrido me atrevería a decir. Suelen ser perfiles generalistas de Seguridad, dedicados a la implementación de herramientas de Seguridad y monitorización y también se encargan de la parte de gestión, haciendo presentaciones, reporting, etc...
Operador del SOC	Estos perfiles trabajan en un SOC. Trabajo por turnos y por lo general con guardias. Su función es monitorizar los sistemas del SOC y analizar y evaluar las alertas e incidentes que se reciben.
Gestor de Riesgos	Estos perfiles no son ciber 100%. Están enfocados a gestionar los riesgos de la empresa, pueden ser IT y, en ocasiones operacionales. En cualquier caso es importante que se alineen con el área de Seguridad para poder aplicar medidas de mitigación a los riesgos que detectan y gestionan.
Pentester	Perfiles muy técnicos que trabajan haciendo pruebas de penetración en las empresas. Muchos profesionales comienzan en este campo, ya que se adquiere un conocimiento ofensivo muy importante, que luego puede convertirse en conocimiento defensivo.
Jefe de Proyectos	Perfil puro de gestión. No tiene por qué ser un experto en Ciberseguridad, pero es muy recomendable cierto background para que sepa lo que está gestionando. Se dedican principalmente a asegurarse del cumplimiento de objetivos en fecha, forma y presupuesto.
CISO	Este es el perfil más alto en términos de autoridad. Suele encargarse de gestionar toda la Seguridad de la compañía. Está a cargo de los equipos, de las tareas y los objetivos del área.

Hay más puestos, más funciones, y más posibilidades. Aquí recojo algunas para que te hagas una idea de hacia dónde puedes ir si decides entrar en este campo.

Si hacemos la escisión “Técnico / Gestión”, te recomiendo nunca lanzarte al 100% a por una u otra variante. Deja siempre, como mínimo un 20% de la otra para ser polivalente, ya que puede ayudarte en más de una ocasión.

Te pongo un ejemplo: decides que quieres enfocar tu carrera hacia el pentesting, un área claramente técnica. En ese caso, distribuye tu conocimiento y habilidades de forma parecida a esto: 80% técnico / 20% gestión. ¿Por qué? Porque, por muy bueno que seas a nivel técnico, en algún momento te va a tocar preparar una presentación, un informe o incluso hablar ante un comité ejecutivo para explicar qué has encontrado y aconsejar cómo poner remedio, por ejemplo. Y para eso, necesitas habilidades de gestión.

Te pongo un ejemplo al revés: si quieres dedicarte a la gestión de proyectos de Ciberseguridad, necesitas un perfil alto de gestión, pero es muy interesante tener un background técnico para saber de qué se está haciendo en el proyecto y, lo que, es más, para que puedas traducir el lenguaje técnico hacia arriba, ya que los comités ejecutivos rara vez quieren enredarse en términos técnicos. Aquí, por ejemplo, un 85% gestión / 15% técnico estaría bien. Dependiendo también de qué complejidad de proyectos vayas a manejar.

7. ¿Qué Estudiar?

Aquí también tienes mucho donde elegir, puesto que han surgido formaciones de Ciberseguridad para todos los gustos. Pero ojo, como todo en esta vida, hay cosas que te servirán a nivel profesional, otras que te servirán a nivel laboral, y otras que no te servirán para nada. Por eso voy a recomendarte las que son, desde mi punto de vista, las mejores formaciones y certificaciones que hay hoy día para cumplir tu propósito de convertirte en un profesional de la Ciberseguridad.

Las hay más generalistas, más técnicas, más de gestión, enfocadas al hacking, a la defensa, al software… Existen un sinfín de páginas y cursos con diferentes rangos de precio, desde la formación gratuita (que no tiene por qué ser mala en absoluto) hasta verdaderas obscenidades que te piden desembolsar miles de euros por una simple certificación.

Vamos a ver una lista de mis favoritas y te cuento un poco sobre ellas:

ISACA CISA	Se trata de uno de los pilares que los profesionales de la Ciberseguridad solemos tener. Te enseña de una forma generalista los dominios de la seguridad y te forma como auditor de los mismos.
ISACA CISM	Un paso adelante con respecto a la anterior. Una vez que te conviertes en auditor, puedes pasar a ser gestor de los sistemas de seguridad.
CompTIA CySA+	Si te interesa el análisis de seguridad, esta es la tuya. Te aportará los cimientos para convertirte en un analista.
CompTIA CASP+	Similar al CISM de ISACA. Te ayuda a entender cómo implementar y gestionar sistemas de seguridad.

CompTIA Pentest+	Como su nombre indica, con esta certificación adquirirás una buena batería de conocimientos sobre el mundo del pentest. Es más técnica que las anteriores.
Cisco CyberOps Associate certification	Esta está más enfocada a las operaciones del SOC. Se centra en la detección y respuesta a amenazas de seguridad.
(ISC)² CISSP	Podríamos decir que es la joya de la corona. Extensa, difícil y cara. Te abrirá muchas puertas profesionales. Te recomiendo no meterte en ella hasta que tengas, al menos, unos 5 años de experiencia en Ciberseguridad.
Offensive Security	Aquí puedes encontrar diferentes certificaciones relacionadas con pentest, aplicaciones web, etc… Una vez más, hablamos de certificaciones orientadas al lado más técnico.
AWS Certified Security - Specialty	Seguridad aplicada a AWS. El curso oficial es muy caro (unos 1.300€ por un fin de semana) y solo te aportará “currículum". Te recomiendo que en lugar de eso, hagas formaciones más baratas en otros portales, te prepares un buen laboratorio para practicar, y vayas directo a la certificación.
Microsoft Certified: Security Operations Analyst Associate	Esta formación es gratuita, solo pagas por la certificación. Si vas a trabajar con Azure (y seguro que va a ser así) es muy recomendable. Orientada a analistas de seguridad.
Microsoft Certified: Azure Security Engineer Associate	Lo mismo que la anterior, solo que orientada a la práctica más pura de Ciberseguridad en Azure.
Google Cloud Security Engineer	Ruta de aprendizaje de seguridad para GCP. Los cursos son gratis, pero como en el resto de proveedores, tendrás que montarte un laboratorio y pagar por los recursos.

También tienes plataformas como Coursera, Udemy, Cybrary o Pluralsight, en las que pagas una suscripción y tienes montones de cursos. En cualquier caso, las certificaciones tienes que pagarlas aparte, y suele ser el lado más caro de las formaciones.

Después, cada fabricante tiene formaciones específicas para sus productos, pero salvo que vayas a utilizarlos de manera asidua en tu día a día no es recomendable que te fijes demasiado en ellas, al menos al principio. Además,

una vez que trabajes con sus productos es muy probable que te ofrezcan esas formaciones de forma gratuita.

Elijas lo que elijas, es muy importante que te formes y que te actualices constantemente, creo que un buen camino es, al principio sacarte un par de certificaciones y después estudiar cursos y aprender mucho en foros, así conseguirás crear una base de conocimientos, mantenerla y hacerla mucho más grande con el paso de los años y la experiencia.

8. Qué nos Depara el Futuro

Afortunadamente, no creo que la burbuja de la Ciberseguridad vaya a explotar de golpe, como sucedió con la inmobiliaria. El horizonte se ve cada vez más tecnológico y los profesionales de la seguridad siempre van a estar ahí. Lo que sí va a suceder es que, en algún punto se deshinchará progresivamente y los menos preparados se encontrarán en un atolladero.

Actualmente las empresas están contratando perfiles de seguridad por encima de sus posibilidades, con sueldos exageradamente altos debido a la necesidad y muchas veces sin tener en cuenta las aptitudes de los candidatos o hacia dónde van a enfocar su propia seguridad. Cuando pase esta tormenta perfecta y haya que regularizar departamentos, tendremos que estar preparados.

Con esto no quiero amargarte el día, estamos en un momento muy dulce y va a durar. Además, se trata de un campo muy bonito, con cientos de posibilidades.

Ten en cuenta todo lo que hay actualmente y todo lo que viene: vehículos eléctricos, el Internet de las Cosas, un mundo hiperconectado… Son todos vectores de ataque y por lo tanto tienen que ser protegidos. Tanto si acabas de empezar tu andadura profesional como si has decidido dar un giro a tu carrera y probar en Ciberseguridad, prepárate bien, estudia, aprende, recíclate constantemente y trabaja duro para ser un verdadero profesional y contribuir a que tengamos un ecosistema más seguro.

Dibujo de portada y páginas diseñado por rawpixel.com / Freepik.