



Raúl Riesco Granadino.

Vicepresidente de Relaciones Institucionales e Inversiones Estratégicas de Telefónica (Eleven paths).

Ingenieros de Telecomunicación y ciberseguridad

Preparados para el cambio

Contar con profesionales bien formados en ciberseguridad es esencial para mitigar los posibles incidentes que puedan afectar, tanto a ciudadanos, como a empresas. Por ello, es imprescindible el fomento y el impulso del talento en nuestro país desde edades tempranas, intentando paliar la falta de profesionales en este sector. **El perfil de Ingeniero de Telecomunicación será una de las opciones aventajadas por su perfil multidisciplinar.**

Estamos viviendo un momento complicado que nadie se podía imaginar a pesar de que años atrás se han dado circunstancias de las que deberíamos haber aprendido más. Por desgracia el riesgo para la salud se ha materializado y ha puesto en práctica nuestra resiliencia como sociedad. La necesidad de respuesta y mitigación ha despertado a grandes personas con principios, valores, solidaridad, creatividad y grandes habilidades y conocimientos multidisciplinarios, dando fruto, en equipo, a soluciones nunca vistas hasta ahora (por ejemplo, *makers* 3D fabricando respiradores o EPIs).

Los tiempos de cambio nos ponen a prueba. Hemos de ser capaces de adaptarnos y aprovechar las oportunidades

de mejora que nos ofrecen. La tecnología y la digitalización son claramente las autopistas para impulsar nuestra economía y la ciberseguridad debe ir por defecto integrada desde su diseño y estar presente en todo el ciclo de vida.

Estas situaciones se dan a diario en el sector de la ciberseguridad al materializarse un riesgo, para el cual podría haber o no, contramedidas previstas. La capacidad de detección temprana y la velocidad de reacción son inversamente proporcionales al daño producido. De igual modo, el talento multidisciplinar es vital para ser resilientes a nuevas amenazas de elevado impacto, como, por ejemplo, aquellas donde se utilizan ataques llamados de día cero (0-day), donde no existe aún una actualización o parche de seguridad.

Y es que 'la seguridad 100% no existe', lo cual no significa que no se pueda hacer nada para reducir o mitigar los riesgos. Muchas organizaciones acababan siendo víctimas de incidentes que podrían haberse evitado, si hubieran invertido a tiempo en medidas de protección básicas, ya que la inversión no es solo cuestión de productos o servicios, también es imprescindible contar con profesionales bien formados en ciberseguridad.

España y la ciberseguridad

Nuestro país destaca especialmente por su talento y por seguir proporcionando al mercado grandes profesionales que tardan poco en fichar por las grandes compañías internacionales por sus habilidades particulares que les

'La seguridad 100% no existe', lo cual no significa que no se pueda hacer nada para reducir o mitigar los riesgos

hacen especiales para resolver problemas complejos que nadie ha resuelto hasta ahora. Se les denomina comúnmente 'hackers'.

Y es que, en situaciones graves, no conocidas hasta el momento, ser capaz de sacar adelante soluciones con los recursos que se tengan a mano, pensando diferente, es algo bastante complicado. A pesar de ello, hay un error común y es pensar que los problemas son siempre técnicos o que con un profesional de esta valía ya no tenemos por qué preocuparnos. Es muy importante contar con un buen equipo cohesionado, complementario y multidisciplinar también en los niveles tácticos y estratégicos. La toma de decisiones, los factores económicos, legales y hasta de recursos humanos son básicos para hacer frente a una gran amenaza.

Perfil multidisciplinar

El Ingeniero de Telecomunicación es un perfil que ha encajado siempre en el sector de la ciberseguridad debido a su carácter multidisciplinar. Estoy seguro

Uno de los problemas más graves de la actualidad es la **falta de conocimientos de desarrollo seguro**, lo cual crea cada día miles de nuevas vulnerabilidades

de que será uno de los grandes contribuidores al éxito del sector y aportará un gran número de profesionales, tanto técnicos, como a nivel de gestión, operativo, pero también táctico y estratégico.

El Ingeniero de Telecomunicación combina elevados conocimientos de telemática, programación (a todos los niveles), electrónica, señales, comunicaciones, gestión, innovación, economía, negocio y hasta bioingeniería. Aun así, creo que sigue siendo necesario introducir de manera contundente conocimientos profundos de ciberseguridad en todas esas asignaturas, especialidades e intensificaciones. Uno de los problemas más graves de la actualidad es la falta de conocimientos de *desarrollo*

seguro, lo cual crea cada día miles de nuevas vulnerabilidades. La sociedad está orientada a multiplicar el número de productos y servicios digitales para mejorar la calidad de vida, lo cual es fantástico, pero éstos deben ser lo más seguros posibles. De igual manera, el 5G, la electrónica asociada a los vehículos conectados con conducción autónoma o los marcapasos conectados no pueden permitirse el lujo de fallos, y mucho menos de vulnerabilidades.

En ciberseguridad hay muchísimas oportunidades y perfiles, desde aquellos orientados a prevenir y predecir incidentes hasta aquellos más relacionados con la respuesta, mitigación y análisis forense. El desarrollo de productos de

Creando un espacio de trabajo seguro

Identifica cada elemento y aplica estos consejos para garantizar la seguridad de la información de tu empresa.

COPIAS DE SEGURIDAD

Te ayudan a proteger la información y a disponer de una versión de respaldo en caso de perder la original. **Aplica la regla 3-2-1.**

DISPOSITIVOS IOT

Los dispositivos inteligentes son cada vez más comunes en las casas, pero si no están bien configurados pueden ser la puerta de entrada a una gran cantidad de amenazas.

DISPOSITIVOS EXTRAÍBLES (USB)

Deshabilita la autoejecución de dispositivos USB. Serás menos vulnerable en caso de que contengan algún fichero infectado.

POST-IT O INFORMACIÓN A LA VISTA

Es importante no dejar a la vista datos relevantes, como claves de acceso.

WIFI/ROUTER

Realiza siempre conexiones seguras. Configura tu router y ten cuidado con las **redes públicas**.

WEBCAM

Mantén el control de tu webcam para evitar fraudes, como la **sextorsión** y el robo de información. **Tapa la cámara** cuando no la estés usando.

IMPRESORA O ESCANER

Es preferible que utilices tus dispositivos. Si usas uno compartido, recuerda **eliminar la bandeja de entrada** cuando termines de utilizarlo.

ACTUALIZACIONES AUTOMÁTICAS

Cada día aparecen nuevas amenazas y vulnerabilidades, por lo que debes mantener el **software** del equipo **actualizado** para hacer frente a dichos riesgos.

SISTEMA BLOQUEADO

Siempre que abandones tu equipo, **bloquea la sesión**. Es un buen hábito para mantener a raya las miradas indiscretas.

DOCUMENTOS Y CARPETAS EN LA MESA

Los documentos en un cajón no están a salvo, mejor mantén la **información cifrada**.

VPN ON

RED PRIVADA VIRTUAL (VPN)

Si tu empresa no te facilita ninguna **VPN** concreta para teletrabajar, te recomendamos que instales una para añadir una capa extra de seguridad a tus conexiones.

¡Sigue estas pautas y disfruta de un entorno de trabajo seguro!

#CiberCOVID19



Mantente al día con nuestras campañas de concienciación para estar informado.

¡Es nuestra mejor defensa!

www.incibe.es | www.osi.es



Demanda de profesionales

Según un análisis de ISC2 se necesita crecer más de un 145% para poder hacer frente a la falta de profesionales del sector actual, estimado en más de cuatro millones de profesionales. La pandemia ha acelerado la digitalización y con ello la gran demanda de trabajadores cualificados en el sector de la ciberseguridad, así como en nuevos nichos de mercado.

McAfee indica que la falta de profesionales es una vulnerabilidad crítica. El 82% de las empresas confirman un *gap* pronunciado. En particular, las principales carencias son de perfiles orientados a la detección de intrusiones, al desarrollo seguro y a la mitigación de ataques.

Para más información:

- <https://www.incibe.es/>
- <https://www.incibe.es/protege-tu-empresa>
- <https://www.osi.es/es>
- <https://www.is4k.es/>
- <https://www.incibe-cert.es/>

ciberseguridad es fundamental para automatizar y simplificar la tarea, pero también para que el resto de productos del resto de sectores incorporen por defecto fuertes estándares de seguridad. Los conocimientos empleados son muy variados, como análisis de inteligencia, ciencia aplicada a los datos, Inteligencia Artificial, telemática, redes, señales y comunicaciones, arquitectura, programación, electrónica, ingeniería inversa, incluso conocimientos de protocolos, de gestión o legales y financieros.

El Ingeniero de Telecomunicación es un perfil que ha encajado siempre en el sector de la ciberseguridad debido a su carácter multidisciplinar

Aquí quiero hacer una reflexión respecto a los niveles directivos y la gran contribución que los Ingenieros de Telecomunicación han aportado en estos niveles desde siempre. Tras mis más de 20 años trabajando en este sector he podido comprobar como el perfil del Ingeniero de Telecomunicación ha sido clave a nivel directivo, especialmente para la transformación de la sociedad. Aún recuerdo con grandísimo respeto y admiración a mi primer mentor, Juan Soto Serrano, Ingeniero de Telecomunicación y expresidente de HP Española.

Como Juan, ha habido grandes Ingenieros de Telecomunicación, empresarios, que han transformado realmente la sociedad a la vez que han sabido inspirar a los futuros líderes y aportar gran valor. Bajo mi punto de vista esto ha sido posible gracias a su profundo conocimiento de lo que tenían entre manos, pudiendo tener una conversación al nivel que sea con cualquier trabajador, técnico o no, pudiendo entender, argumentar o debatir cualquier idea. A este tipo de directivos los denominó 'directivos Full Stack' y me parecen claves, aún más, si cabe, para la gran transformación que estamos sufriendo y para garantizar un fuerte liderazgo frente a la elevada competitividad internacional en el sector de la ciberseguridad.

En mi paso por el Instituto Nacional de Ciberseguridad (INCIBE) destacaría la labor que se está realizando desde hace ya muchos años en despertar la vocación en este sector de pleno crecimiento y empleo, así como en identificar y detectar el mejor talento desde edades tempranas junto con grandes socios estratégicos tanto públicos como privados.

Así, iniciativas como *CyberCamp*, *CyberOlympics* y el *European Cybersecurity*

Challenge permiten conocer el gran potencial de nuestros jóvenes de manera temprana mediante retos y pruebas de habilidad para nutrir al sector a medio y largo plazo. Por otro lado, programas más especializados, como el *Cybersecurity Summer Bootcamp*, el programa *#include* o el programa *SAPROMIL* del Ministerio de Defensa, están enfocados a reorientar carreras profesionales a corto plazo.

Son tantas las opciones, perfiles y puestos de trabajo que recomiendo ver charlas y talleres y de ahí iniciar nuestro itinerario formativo buscando aquella formación reglada y no reglada que más nos acerque a esos perfiles, considerando, especialmente como algo clave, el autoaprendizaje.

La inversión en certificaciones es importante ya que se valora bastante en el sector. Mi recomendación, no obstante, es que analicemos cuales se valoran más investigando las ofertas de trabajo.

A modo de conclusión

Las habilidades son claves y por eso no recomiendo planes formativos orientados y guiados en exceso, ya que es bastante improbable que las situaciones complejas se resuelvan tirando de un manual. Conozco a grandes profesionales en este sector, autodidactas, aunque todos ellos reconocen que les hubiera venido genial haber ido a la universidad para tener un perfil más multidisciplinar.

En resumen, el futuro es muy prometedor para el perfil del Ingeniero de Telecomunicación, especialmente por esa faceta multidisciplinar, lo cual creo sinceramente que es un privilegio en este entorno de tal incertidumbre. Solo hay un problema y es que como bien dice Víctor Küppers, el conocimiento y la experiencia suma, pero la actitud multiplica y con signo. ¿Quién querría a alguien con grandísimos conocimientos, pero con actitud negativa? Nadie. Como decía Michael Jordan, el talento gana partidos, pero la inteligencia y el trabajo en equipo ganan campeonatos. ■