



Emilio Rodríguez Priego.

Ingeniero de Telecomunicación (UPM) y Doctor en Ingeniería Informática (UR). Auditor TIC en Gobierno de la Rioja y profesor de Seguridad en la Universidad de la Rioja.

Se buscan Telecos para Administraciones ciberseguras

Las Administraciones Públicas ofrecen a los profesionales de la Ingeniería de Telecomunicación un entorno de trabajo estimulante con importantes retos donde desarrollar sus aptitudes para **abordar proyectos de carácter transversal como el de la implantación de la ciberseguridad.**

Durante las últimas décadas la sociedad ha experimentado profundos cambios como consecuencia del desarrollo y el progreso, afectando a diversos sectores como la economía, la sanidad, la agricultura, la industria, las relaciones sociales, etc. Uno de los factores transversales que ha propiciado estos cambios son las TIC, cuyo crecimiento exponencial ha seguido lo que Ray Kurzweil denominó la 'Ley de rendimientos acelerados', considerada como una generalización de la conocida 'Ley de Moore'. Es importante no perder de vista este enfoque, porque nos permitirá entender y contextualizar el momento que estamos viviendo actualmente y las expectativas de cambios en el futuro.

El valor del IT

En este contexto, determinados profesionales son llamados a ser los actores principales de este desarrollo tecnológico, especialmente aquellos cuya formación y experiencia se conoce como STEM (siglas en inglés de Ciencia, Tecnología, Ingeniería y Matemática). Dentro de la ingeniería destaca la formación en Teleco, por ser

las TIC uno de los factores principales de esta transformación tecnológica.

Podemos pensar que este protagonismo de la Ingeniería de Telecomunicación se refiere principalmente al aspecto técnico. Sin embargo, el profesional de las TIC, y concretamente el Teleco, debe ofrecer también competencias no técnicas para seguir liderando este cambio. En una de las tablas que acompaña este artículo, he destacado las principales competencias que, según mi experiencia y conocimientos, diferencian al profesional de ingeniería, más concretamente al Teleco, y a las que nos referiremos más adelante al analizar el papel que juega el Teleco en la Administración Pública (AA.PP.) y en particular en los proyectos de ciberseguridad.

Sector público versus sector privado

Estas cualidades del Teleco permiten que sea una de las profesiones más demandadas en muchos sectores, tal como refleja el informe 'Perfil del Ingeniero de Telecomunicación' presentado por el COIT y la AEIT en 2017, donde

En los últimos años el creciente uso de las TIC ha propiciado el aumento de los ataques informáticos a personas y organizaciones, incluidas las AAPP

PRINCIPALES COMPETENCIAS DEL IT

CIT1	Profundos conocimientos de las tecnologías de la información y las comunicaciones
CIT2	Visión global de los problemas
CIT3	Predisposición para aprender y estar al día en nuevos conocimientos
CIT4	Habilidad para adaptarse en entornos cambiantes
CIT5	Capacidad para resolver problemas complejos en contextos adversos
CIT6	Espíritu investigador, emprendedor e innovador
CIT7	Capacidades de organización y planificación
CIT8	Aptitudes para la comunicación y enseñanza de conocimientos
CIT9	Capacidad de liderazgo y de trabajo en equipo
CIT10	Buenas aptitudes para el análisis

CAPACIDADES DEL TELECO Y REQUISITOS DEL ESQUEMA NACIONAL DE SEGURIDAD

Art. 5 Seguridad como un proceso integral	CIT2
Art 6 Gestión de la seguridad basada en los riesgos	CIT10
Art 13 Análisis y gestión de los riesgos	
Art. 43 Categorías	
Art 7. Prevención, reacción y recuperación	CIT5
Art. 9. Reevaluación periódica	CIT3, CIT4, CIT5, CIT6
Art. 26 Mejora continua del proceso de seguridad	
Art. 12 Organización e implantación del proceso de seguridad	CIT7, CIT9
Art. 14 Gestión de personal	CIT8
Art. 15 Profesionalidad	CIT1

se indica que la Administración Pública y Defensa es el sector preferido por el 20% y uno de los que más crece.

Pero ¿cuáles son las principales diferencias que se va a encontrar un Teleco en la Administración Pública comparada con el sector privado? En la tabla adjunta, se relacionan las principales diferencias (pueden variar según el tipo de administración o de empresa).

Pueden observarse diferencias importantes. El puesto en una Administración Pública es generalmente estable, pero la estrategia de la organización suele cambiar cada legislatura. Esto implica que el empleado público debe adaptarse con frecuencia a cambios en

el enfoque que el gobierno correspondiente tiene sobre las TIC.

La entrada en la organización también es muy diferente. En la empresa privada la contratación es más flexible y la selección se realiza generalmente en base al currículo y a una entrevista personal. Sin embargo, en la Administración Pública se hace generalmente mediante una convocatoria pública regulada por normativa dando lugar a una oposición con pruebas orales y/o escritas.

En lo que respecta a los recursos para llevar a cabo los proyectos también existen diferencias relevantes. Una empresa privada, en general, dimensiona libremente sus recursos en función de

su evolución económica invirtiendo y/o contratando nuevo personal para mejorar su rentabilidad. Por el contrario, la Administración Pública está sujeta a unos presupuestos aprobados anualmente. Esto puede impedir actuar con flexibilidad y añade una carga administrativa elevada dificultando el desarrollo de los proyectos.

Si comparamos estas diferencias con las aptitudes indicadas anteriormente para los profesionales de Telecomunicación, vemos que la capacidad de aprender nuevos conocimientos, sobre todo en legislación y cuestiones administrativas (CIT3) y su facilidad para adaptarse en situaciones cambiantes (CIT4), permiten que estos profesionales sean muy bien valorados en la Administración Pública. Por otro lado, su espíritu innovador (CIT6) y sus aptitudes para la comunicación hacen que también sean apreciados para el asesoramiento a los dirigentes políticos que planifican la acción de gobierno en las TIC.

Ciberseguridad en la Administración Pública

Por la propia naturaleza de las TIC, la mayoría de los proyectos que debe abordar un Teleco en la Administración Pública tienen un carácter transversal: redes de comunicaciones, infraestructura de centros de proceso de datos, ciberseguridad, administración electrónica, etc. En este contexto, la aptitud más necesaria es la visión global (CIT2), junto con la de tener una visión de futuro en situaciones de cambio continuo (CIT4).

Entre los proyectos transversales, el de ciberseguridad es especialmente importante. En los últimos años el creciente uso de las TIC ha propiciado el aumento de los ataques informáticos a personas y organizaciones, incluidas las AA.PP.

La ciberseguridad en una Administración Pública es un reto que exige aún más de las capacidades que hemos señalado para los proyectos transversales, ya que no se puede abordar únicamente desde un punto de vista técnico.

DIFERENCIAS SECTOR PÚBLICO Y PRIVADO PARA UN IT

	EMPRESA	ADMINISTRACIÓN PÚBLICA
Selección de personal	C.V. y entrevista personal	Titulación y examen
Experiencia laboral	Se valora en la selección	No se requiere en general
Dirección	Generalmente formada por directivos con experiencia previa	Personal con cargo político elegido por el gobierno correspondiente
Estabilidad laboral	Diversa	Mayoritariamente estable
Movilidad geográfica	Establecida según las necesidades de la empresa	Limitada por la normativa
Movilidad funcional	Establecida según las necesidades de la empresa	Limitada por la normativa
Ventas	Productos y/o servicios	Servicios públicos
Ingresos	Por venta de productos y/o servicios	Mayoritariamente por impuestos
Inversiones y gastos	Restringidos por la evolución de las ventas	Restringidos por los presupuestos propuestos por el gobierno correspondiente
Estrategia de la organización	Establecida por la dirección. Generalmente estable, aunque condicionada por la evolución de la rentabilidad	Sujeta a cambios cada legislatura
Adquisiciones de bienes y/o servicios	Libre según los criterios de la empresa	Sujeta a la compleja legislación sobre contratación pública

co, sino que los aspectos organizativos y normativos tienen una importancia incluso mayor. Esto es debido a la aplicación del principio de seguridad conocido como ‘participación universal’ (todos los usuarios tienen responsabilidad en la seguridad) y el del ‘eslabón más débil’ (la seguridad de un sistema es la de su punto más débil, y éste suele ser el factor humano).

Precisamente la normativa es una de las bases que sustenta a la ciberseguridad. Normas como la ISO 2700X de ámbito global, el Reglamento General de Protección de Datos de ámbito europeo o el Esquema Nacional de Seguridad (ENS) de ámbito español, son fundamentales para abordar la seguridad, especialmente en las AA.PP. De éstas la que mejor integra la aplicación de las demás es el ENS. En el cuadro adjunto se relacionan las capacidades del Teleco con los requisitos exigidos en el Es-

quema Nacional de Seguridad. Como se puede observar en dicho cuadro, el cumplimiento de la normativa por parte del Teleco implica poner a prueba todas sus capacidades, pero además debe hacerlo trabajando conjuntamente en equipos multidisciplinares.

Con vistas a futuro y según la ‘Ley de Rendimientos Acelerados’, la tecnología seguirá avanzando tanto para los atacantes como para los profesionales que deben prevenir, corregir o recuperarse de sus ataques. La mejora continua a la que hace referencia el Esquema Nacional de Seguridad indica que se trata de un proceso vivo que presenta continuamente nuevos retos: la aplicación de la Inteligencia Artificial a la ciberseguridad, la seguridad en *Blockchain*, la protección de datos personales en un entorno cada vez más global y conectado, la seguridad del Internet de las cosas, los efectos de la computa-

ción cuántica en la ciberseguridad, etc. Se trata sin duda de retos cada vez más estimulantes para el profesional de la Ingeniería de Telecomunicación en la Administración Pública. ■

¿Qué aporta el Teleco en ciberseguridad a la AAPP?

- Capacidad técnica en TIC (CIT1).
- Conocimientos en normativa, que ha debido adquirir al incorporarse al sector público (CIT3).
- Capacidad para gestionar y coordinar las acciones del conjunto de la organización con una visión global (CIT2).
- Capacidad para estar al día a nivel técnico (CIT3) y para afrontar cambios (CIT4) que le permitirá abordar uno de los requisitos de la ciberseguridad: la revisión continua para enfrentarse a nuevas amenazas, modificaciones en la normativa, etc.

La tecnología seguirá avanzando tanto para los atacantes como para los que deben prevenir y corregir sus ataques