



HACKING DETECT



Álvaro Ubierna Alonso.

Socio fundador y COO de RKL integral. Decano territorial del COIT en el País Vasco.

Carlos Prieto Lezaun.

Director-Consultor Senior Ciberseguridad SSHTeam. Vocal de la AEIT.

Idoia Uriarte Letamendi.

CISO Grupo Euskaltel.

Ciberseguridad Necesidad esencial para una sociedad en transformación... digital

El proceso de Transformación Digital que afecta a la sociedad desde hace décadas –con el importante impulso recibido a raíz de la pandemia y el confinamiento– pone de manifiesto la necesidad de considerar la **ciberseguridad como una necesidad básica de nuestras empresas y de nuestra vida en general**. En este escenario, los Ingenieros e Ingenieras de Telecomunicación debemos conquistar el papel de liderazgo que nuestra formación y nuestras capacidades avalan.

Indudablemente recordaremos este año 2020 como aquel en el que nuestras vidas cambiaron radicalmente. Un año en el que apareció en escena la pandemia del coronavirus y convirtió, de la noche a la mañana, nuestro día a día en una de esas películas de catástrofes exageradas, tan típicas de la sobremesa de los domingos.

¿Quién se habría imaginado hace ocho meses que nuestra sociedad se vería obligada, y sería capaz, de confinarse en sus casas durante tres meses?

Es cierto que el cambio más visible es que ahora todos usamos mascarilla en los lugares públicos. Pero con toda seguridad es mucho mayor el impacto que ha tenido a nivel psicológico: esta pandemia ha generado una gran incertidumbre en nuestro entorno y está poniendo en entredicho muchas actividades que antes dábamos por seguras: abrazar a nuestros mayores, estrechar la mano a un cliente, cantar y bailar en una fiesta, la estabilidad del puesto de trabajo... en fin, la lista sería interminable.

Es, desde un punto de vista antropológico, un auténtico torpedo a la línea de flotación de unas de las principales necesidades básicas del ser humano: la seguridad.

Seguridad: necesidad prioritaria

Porque precisamente la seguridad (de momento no le añadiremos el prefijo 'ciber') ya fue catalogada por el psicólogo estadounidense Abraham Maslow en 1934, en su teoría de 'la Jerarquía de Necesidades', dentro del segundo nivel de importancia de las personas, y únicamente por detrás de las necesidades fisiológicas como el respirar, la alimentación, el descanso o la reproducción.

La seguridad es la base sobre la que construimos nuestras relaciones socio-afectivas de familia y amistad, el pilar que nos permite disfrutar de nuestro hogar, nuestra ciudad y nuestro trabajo, y, entre muchas otras cosas, la garantía que nos anima a promover y a invertir en los negocios que mueven la economía.

Dependiendo del ámbito en el que nos movamos, a la seguridad se le pueden poner apellidos que la acoten, tales como seguridad ciudadana, seguridad laboral, seguridad industrial, seguridad jurídica, seguridad informática, seguridad nacional o incluso, estirando el concepto, 'la seguridad social', refiriéndose en todo caso a las condiciones que garantizan el buen funcionamiento de nuestra 'vida normal'.

Y hasta aquí llega el discurso de manera similar al que podríamos haber hecho en los años 90 del siglo pasado. Pero desde entonces hasta ahora la revolución de la información iniciada en la segunda mitad del siglo XX ha conducido a nuestra sociedad, como bien todos sabemos, a un continuo y acelerado proceso de Transformación Digital en el que todavía estamos inmersos. Proceso inacabado que está cambiando radicalmente las reglas del juego sociales y económicas de las generaciones anteriores y sobre el que los profesionales de la Ingeniería de Telecomunicación tenemos mucho que decir.

Le añadimos el prefijo 'ciber'

En este mundo digital en el que nos movemos ya hace unas décadas que el concepto de seguridad de Marlow se actualiza necesariamente con el prefijo 'ciber'. La ciberseguridad se ha convertido en una nueva dimensión de la seguridad que, con un incontestable impacto transversal, afecta a cualquier aspecto de nuestra vida personal, de la sociedad y de la economía.

Pero aquí surge la incongruencia de que, a pesar de su gran importancia y de su 'omnipresencia', el hecho de referirse al mundo del ciberespacio, ese

mundo no real, no físico (hablando de físico como lo tangible), convierte a la ciberseguridad en una disciplina tremendamente complicada de gestionar, tanto a nivel técnico como de asimilación social.

Como ejemplo clarificador de este punto, basta con fijarse en detalles como que hoy en día a nadie se le ocurre dejar el coche con las llaves puestas y las ventanillas bajadas aparcado en medio de una ciudad, y nadie deja la puerta de su casa abierta de par en par -o cerrada con un trozo de cello-. Sin embargo, es de sobra conocido cuantos sistemas informáticos siguen estando desprotegidos o bajo contraseña del tipo '1234'. Una importante consultora internacional cifraba en el 90% el porcentaje de las contraseñas de los usuarios de todo el mundo que son vulnerables a los ataques de los ciberdelincuentes.

La ciberseguridad es una disciplina tremendamente compleja y en constante evolución que se integra en todos los ámbitos de nuestra vida y requiere profesionales muy preparados y competentes. Y los Ingenieros de Telecomunicación (IT) cumplimos a la perfección con esta necesidad, por formación y capacidades.

En esta revista que tienes en tus manos -o, la gran mayoría, en tu pantalla- queremos destacar algunos de los aspectos más importantes de la ciberseguridad, pero, sobre todo, hacer énfasis en el importante papel que jugamos los Ingenieros e ingenieras de Telecomunicación en este campo.

Nos acompañan en las páginas siguientes un puñado de compañeros

La ciberseguridad es una disciplina tremendamente compleja y en constante evolución que **requiere profesionales competentes. Y los IT cumplimos a la perfección con esta necesidad**



con mucha experiencia en el sector, con perfiles muy diversos, que nos ofrecerán aspectos muy variados de la ciberseguridad y el rol de nuestra profesión. A todos ellos les agradecemos de corazón su dedicación en este especial de Bit.

Nuestro mundo es ciberfísico

Quizás haya a quien este término de ‘mundo ciberfísico’ aún le suene un poco raro, pero lo cierto es que en la actualidad ya no es posible en la mayoría de las situaciones de nuestra vida cotidiana diferenciar el mundo físico tradicional de nuestros mayores del mundo virtual o ciber de nuestros hijos.

Gran parte de los trámites que hace dos décadas nos obligaban a desplazarnos a lugares en concreto y a utilizar elementos físicos, como papeles, fotografías o dinero en efectivo, hoy los hacemos gracias a nuestros dispositivos móviles desde cualquier rincón del planeta y sin importar la hora del día: compras, comunicación con los seres

queridos, acceso a la información actualizada, ocio, trabajo, formación...

Unas páginas más adelante nuestro compañero Pablo López nos mostrará, gráficamente y con ejemplos reales, esta interacción entre las amenazas ciberfísicas y el mundo real de las infraestructuras críticas. Y, por su parte, Enrique Cobo nos va a explicar cómo ese 5G del que tanto hablamos ya está pensado desde su diseño, afortunadamente, como una base segura de comunicaciones sobre la que vertebrar todos los servicios que necesite nuestra sociedad.

Haciendo el esfuerzo de buscar algo positivo en la experiencia de la pandemia de la COVID-19 que estamos sufriendo, podríamos destacar como en este segundo trimestre del año 2020 la transformación digital de nuestra sociedad y de nuestra economía ha tenido un desarrollo mayor que el que se ha observado en los últimos 15 años, y donde los profesionales del mundo TIC hemos tratado de evangelizar para que así fuera.

En este segundo trimestre la transformación digital ha tenido un desarrollo mayor que el que se ha observado en los últimos 15 años

En estos meses, el teletrabajo, la teleformación, el ocio digital, las compras online y las redes sociales nos han permitido soportar el confinamiento con niveles de calidad de vida notables dentro de la incomodidad de la situación.

Además, los sistemas TIC se han demostrado imprescindibles para comunicar a la sociedad la información sobre la situación y las medidas a adoptar, así



como ayudar en el seguimiento y desarrollo de la pandemia o el número y la evolución de personas infectadas.

En este punto, queremos aprovechar para reconocer y agradecer el trabajo ímprobo de los profesionales del sector de las telecomunicaciones que con muchísimo esfuerzo y buen hacer ha permitido que nuestra vida pudiera seguir funcionando a pesar de las circunstancias excepcionales.

Pero no podemos olvidar que el teletrabajo y la teleformación que se han implantado de forma generalizada en las empresas y en nuestra sociedad en general lleva asociados una serie de riesgos con respecto a la ciberseguridad. Hemos visto que nuestras instituciones y empresas no estaban en su mayoría preparadas para esta situación (¿quién lo podría prever?) y que la puesta en marcha de forma precipitada de estos sistemas ha mostrado tremendas carencias en este aspecto.

Generalmente, y dentro de su complejidad, es más sencillo montar los sistemas (ordenadores, servidores, VPN, firewalls, copias de seguridad, etc.) que modificar los procesos de trabajo y formar y concienciar a las personas. Estas tareas no se pueden improvisar y requieren una adecuada previsión.

Ahí es donde entra el famoso triángulo de la seguridad, y a la hora de adoptar medidas de seguridad –o ciberseguridad– es donde debe cuidarse el equilibrio entre las personas, la tecnología y los procedimientos, de tal forma que una persona esté concienciada, tenga las herramientas necesarias y sepa cómo utilizarlas. De otra manera no se conseguirán los objetivos previstos.

Este proceso de transformación digital refuerza la integración del mundo ciberfísico, en el que nuestras labores del día a día se combinan entre presenciales y telemáticas y en el que empiezan a surgir amenazas, porque los delincuentes lo saben e intentan explotarlas. Por eso, ahora más que nunca, realmente siempre, es imprescindible reforzar la ciberseguridad de las instituciones y de las empresas, sean del tamaño que sean, empezando por el eslabón más débil, que es la formación e información a sus trabajadores y usuarios de los riesgos y buenas prácticas en ciberseguridad.

Debe cuidarse el equilibrio entre las personas, la tecnología y los procedimientos. De otra manera no se conseguirán los objetivos previstos

Más adelante, en su artículo, Samuel Álvarez nos hace una brillante exposición del impacto que la ciberseguridad tiene en nuestro devenir diario y en el de nuestras empresas.

Y no es por ser agoreros, pero mucho nos tememos que algunos de los efectos de esta pandemia hayan llegado para quedarse y modifiquen ciertos hábitos de nuestra sociedad restando peso a las relaciones físicas y favoreciendo el distanciamiento y el uso de medios electrónicos. Así que más nos vale tomárnoslo en serio y prepararnos adecuadamente para vivir y disfrutar, pero con seguridad, de este mundo ciberfísico.

El rol imprescindible de los telecos

Ya comentábamos antes la importancia de resaltar la figura de Ingenieros e Ingenieras de Telecomunicación como artífices imprescindibles dentro de este marco de actuación de la ciberseguridad. Y no lo decimos únicamente con un interés meramente corporativista –aunque un poco también– sino con el

convencimiento absoluto de que los conocimientos específicos de nuestra formación nos convierten en el tipo de profesionales idóneos para esta tarea.

La capacidad de análisis, resolución de problemas, adaptación y conocimiento de la tecnología que tenemos los Ingenieros de Telecomunicación hacen que nuestro perfil sea el idóneo para especializarnos y liderar la transformación digital, y dentro de ella, ¿por qué no?, también la ciberseguridad.

En uno de los artículos de este especial sobre ciberseguridad, Emilio Rodríguez Priego nos plantea una detallada exposición de las principales competencias del IT, que muestran con claridad las razones de la necesidad de que seamos los Ingenieros de Telecomunicación quienes libremos la lucha en este sector.

Somos conscientes de que partimos de la desventaja de que actualmente la sociedad identifica muchas veces más al ingeniero informático como el líder en esta área de la ciberseguridad, y, lamentablemente, ocurre lo mismo en otros campos como el Big Data o la Inteligencia Artificial.

Pero si analizamos brevemente dónde residen los riesgos más importantes en el mundo de la ciberseguridad veremos que no están tanto en los sistemas informáticos en sí mismos como en los sistemas de comunicaciones que los unen.

Si lo comparamos con el sector del motor y del tráfico, los riesgos en ese mundo no están tanto en que fallen los vehículos estando parados y solos, que ocurre a veces, sino en la amenaza de los conductores irresponsables, las carreteras mal conservadas, la falta de accesos redundantes o debidamente dimensionados en las ciudades o el

incumplimiento de las normas de circulación. Lo que equivale a nuestros protocolos y enlaces de fibra y radio.

Obviamente, no se está planteando que solo seamos los IT los únicos que trabajemos en el área de la ciberseguridad, porque lo que se necesitan son equipos multidisciplinares de profesionales TIC y de otras áreas, ya que la complejidad y diversidad de amenazas y problemas que surgen en ese sector es cada vez más amplia y diversa. Pero indudablemente los Ingenieros de Telecomunicación tenemos una visión muy amplia y especializada de estos sistemas que nos convierten en piezas fundamentales dentro de estos equipos.

Por otro lado, también es importante que estos grupos de trabajo estén formados por profesionales de diferentes edades y composición de género que aporten visiones y experiencias complementarias.

La globalización se ha convertido, como muchas otras revoluciones tecnológicas aparecidas a lo largo de la historia, en un arma de doble filo que facilita, por un lado, el desarrollo de una sociedad moderna y de numerosos servicios que mejoran nuestra calidad de vida como hace décadas ni siquiera habríamos podido imaginar y, por otro, facilita a la vez que los ataques y delitos se cometan desde cualquier lugar del planeta aprovechando las distancias y diferencias culturales y legales para lograr un alto nivel de impunidad.

Nuestro colega Raul Riesco hará hincapié, más adelante en su artículo, en la apremiante necesidad de profesionales cualificados que ha surgido en el sector de la ciberseguridad, así como en nuevos nichos de mercado con la aceleración de la digitalización que ha traído la pandemia. ■

Un área profesional con mucho futuro

Como conclusión de todo lo expuesto queremos incidir en el importante papel que desde nuestra profesión podemos realizar para mejorar los niveles de seguridad de nuestra sociedad y nuestra economía, especialmente en el mundo de la ciberseguridad.

Con ese objetivo, el COIT, entre otras medidas, ha puesto en marcha hace unos años ya un grupo de trabajo centrado en la defensa y la seguridad, donde la ciberseguridad tiene un peso importante, trabajando sobre aspectos variados en los últimos años al ritmo que marca la realidad tecnológica y la reglamentación.

Y en la línea de ganar esa visibilidad social y profesional para nuestra profesión, nuestro colegio participa activamente entre otros foros en el Comité CTN320 de AENOR, sobre Ciberseguridad y Protección de Datos Personales.

Cuando se habla de las grandes verticales tecnológicas de los últimos años con mayor impacto en nuestra sociedad aparecen conceptos como Big Data, IoT, Robótica, Ciberseguridad, Inteligencia Artificial, etc. Si bien somos conscientes de que los telecos no podemos especializarnos en todas ellas, creemos que especialmente en el mundo de la ciberseguridad debemos reafirmar nuestra posición y liderazgo, estando como estamos muy capacitados para desarrollar un papel imprescindible e importante ganándonos el reconocimiento como colectivo.

La ciberseguridad se ha convertido en una nueva dimensión de la seguridad que afecta a cualquier aspecto de nuestra vida