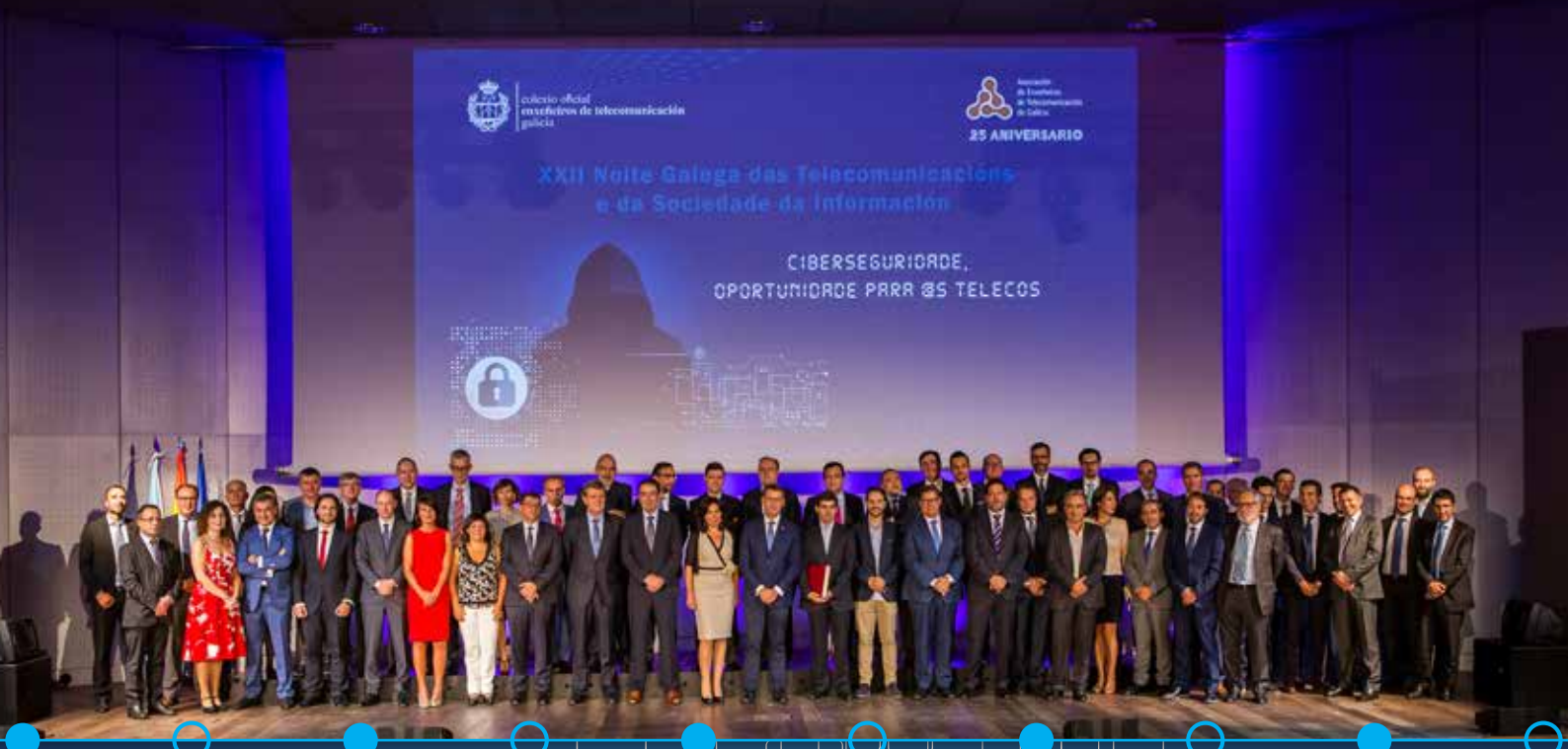
# A Nosa Rede

Venres, 17 de novembro do 2017

## XXII Noite Galega das Telecomunicacións e da Sociedade da Información 2017




colexio oficial
enxeñeiros de telecomunicación
galicia

Asociación
de Enxeñeiros
de Telecomunicación
de Galicia

25 ANIVERSARIO

CIBERSEGURIDADE,

OPORTUNIDADE PARA @S TELECOS

A NOSA REDE



colexio oficial enxeñeiros de telecomunicación galicia

Rúa Juana de Vega, 4 – 1º I
15003 A Coruña
T: 981 919 300 F: 981 919 301
administracion@coetg.gal

*Edita:*

Asociación de Enxeñeiros de Telecomunicación de Galicia

Escola de Enxeñaría de Telecomunicación (EET)
Campus Lagoas-Marcosende s/n
36310 Vigo - Pontevedra
T: 986 465 234 F: 886 125 996
administracion@aetg.gal

ISSN: 1699-3861



## DIRECTORIO PROFESIONAL DE GABINETES E ENXEÑEIROS DE TELECOMUNICACIÓN

**ACBIA SOLUCIONES S.L.U.**
**FAUSTINO CASTRO SANJORGE**
Nº Colegiado: 12363
Tfno: 981650870 - Movil: 677163247
fcastro@acbia.com / acbia@acbia.com
Consult. Estratégica, Conectividad/ Comunicaciones, A.Técnica

**AEROWI**
**RAMÓN FERNÁNDEZ REGO**
Nº de colexiado: 18.269
Teléfono: 688907132
27619 Sarria (LUGO)
info@aerowi.es
www.aerowi.es
Especializados en proxectos de redes sen fíos

**ALFONSO MOREDO ARAÚJO**
Nº de colexiado: C16749
Teléfono: 656162452
Vigo
alfonsomoredo@coit.es
Consultoría en Sistemas de Gestión de I+D+i para PYMES

**BALSAINGENIERIA SL,**
**ATELIER METROPOLITANO SL**
**JOSE LUIS BALSA CALVO**
Nº de colexiado:2.225
**JOSE FRANCISCO BALSA GONZALEZ**
Nº de colexiado:17.767
981907976
Rúa Pla y Cancela 27. 15005 A Coruña
oficina@balsaingenieria.com
www.balsaingenieria.com
www.ateliermetropolitano.com
INGENIERIA DE TELECOMUNICACIÓN, ARQUITECTURA E INMOBILIARIA

**BOADO INTEGRA INGENIEROS**
**ALFONSO SAAVEDRA BOADO**
Nº Colegiado: 9220
Santiago de Compostela
Tfno: 981 571284 teleco@boado.com
Proyectos de ICT, Acústica, TDT, Gap-Fillers, WiMax

**CESÁREO GARCÍA RODICIO**
Nº Colexiado: 8038
www.cesareox.com
+34 988 980044
Sistemas de Información

**DOMOTECH, SL**
**MARIO REBOREDA PUIME**
Nº de colexiado: 8518
Teléfono: 986229506
Vigo, Pontevedra
info@domotech.es
www.domotech.es
ICT, Consultoría, WSN, Redes

**DUOTELECO**
**JOSÉ ANTONIO GARRIDO CIMADEVILA**
Nº de colexiado:6378
Teléfono: 986866658
R/ Luis Otero, 2 bajo dcha
36005 Pontevedra
info@duoteleco.es
www.duoteleco.es
Operador WISP internet rural
Redes WIRELESS. Ingeniería

**EVENTIAM INGENIEROS, S.L.**
**MARÍA E. BALTAR CARRILLO**
Nº colegiada: 6470
**JOSÉ ANTONIO CENTOIRA GARCÍA**
Nº colegiado: 15090
C/Doctor Cadaval, 33 – Ofic. 2º b
33202 Vigo • Tfno: 986 120 106
www.eventyam.com
Campos electromagnéticos. Ruido. Termografía. Proy./Certif.

**GIZA INGENIERÍA S.L.**
**LUIS MANUEL SÁNCHEZ GARCÍA**
Nº colegiado: 6179
Lugar da Granxa 15B Mondego
15168 Sada - A Coruña
Tfno: 881991447, giza@gizaingenieria.es
Servicios de Ingeniería. Proyectos Direcciones de Obra. ICT

**IRIX GALICIA S.L.**
**CARLOS MOSQUERA MONTERO**
Nº colegiado: 12.589
C/Joaquin Cotarelo 2 bajo 15008 A Coruña
Tfno: 981912305 • Fax: 981065200
irix@irix.es www.irix.es
SW a medida. Diseño web, Inst. y Manten. Redes, Recup. Datos

**JAVIER FERNÁNDEZ FRAGA**
Colegiado nº 5039
C/Recatelo 21 - 2º A - 27002 - LUGO
Tfno: 982100609 javierfraga@coit.es
Proyectos, medidas radioeléctricas e informes periciales.

**JESÚS AMIEIRO BECERRA**
Nº colexiado: 13.432
O Porriño - Pontevedra
Tfno: 630615609
jesus@jesusamieiro.com
http://www.jesusamieiro.com
Informes periciales, consultoría TIC, software a medida, ICT

**JULIO PÉREZ FORMOSO**
Nº Colegiado: 6252
C. Ramón Cabanillas, 13, 1º B - 32004 Ourense
Tfno/Fax: 988391519 • Móvil 619419689
juliopf@iies.es www.julioformoso.es

**KASTEL INGENIERÍA**
**JOSÉ RAMÓN PÉREZ CASTELAO**
Nº colegiado: 14226
La Campiña, 114 - 27192 Lugo
Tfno: 685887625
info@kastel.es
www.kastel.es
Certificaciones,ICTs,Estudios Viabilidad,Titulos Habilitates

**MARÍA L. HIDALGO SOTELO**
Nº colegiada: 7191
A Coruña
Tfno: 630 940 650
mhidalgo@coit.es
Gestión innovación.
Firma electrónica. Herramientas SW. ICTs

**PC CARRIER, S.L**
**XOSÉ ANTONIO DOLDÁN PEDREIRA**
Nº colexiado: 12271
Tfno: 981 140 800 x.doldan@pcarrier.com
Formación TIC, Inst. Networking, ERP/CRM, Sistemas CAD/CAM

**PROITEC GESTIÓN INTEGRAL S.L.U.**
**ADRIÁN RODRÍGUEZ FERNÁNDEZ**
Nº de colexiado:17.284
Camiño Verde 23 Bis Entresollado, 27004 - Lugo
Tfno: 646167473
adrian@proitec-cti.com
www.proitec-cti.com
Consultoría Técnica de Construcción, Actividades e Instalacións

**ROGELIO MARTÍNEZ TEIJEIRA**
Nº Colexiado: 8328
Tfno: 625192714 rm_teijeira@yahoo.es
ICT's, Redes de Datos, Instalacións de seguridade, megafonía

**SIM SL**
**PABLO SOTO CID**
Nº de colexiado:14.564
**JOSÉ MANUEL SOTO VAZQUEZ**
Nº de colexiado:2.044
C/ Rodríguez de Vigurí, nº 24 Bajo
15703, Santiago de Compostela (A Coruña)
981 103 427
s-i-m@s-i-m.es
www.s-i-m.es
Ingeniería, Consultoría, Proyectos y Direcciones de obra

**SMARTEL GESTIÓN Y SERVICIOS, S.L.**
**MANUEL BERMEJO PLANA**
Nº de colexiado:8.681
Tel.: 644 30 20 13
Sanxenxo (Pontevedra)
direccion@smartelgestion.com
www.smartelgestion.com
Radiocomunicaciones, informática, TDT, Gap-fillers, proyectos y direcciones de obra

**SONEN, CENTRO DE ACÚSTICA E SERVIZOS DE TELECOMUNICACIÓNS, S.L.**
**CÁSTOR RODRÍGUEZ FERNÁNDEZ**
Nº Colexiado: 15080
Vial Centro Comercial, Parcela 11
32710 Pereiro de Aguiar - Ourense
Tfno: 652 770 034
info@sonen.es www.sonen.es
Consultoría en acústica arquitectónica e medioambiental

**URBAN LAB MADRID BUSINESS CENTER**
**AUGUSTO DE ARAÚJO TRIGO**
Nº de colexiado: C01743
Teléfono: +34 609408583
Manuel Tovar, 42- 28034 MADRID
adearaujo@urbanlabmadrid.com
www.urbanlabmadrid.com
Centro de Negocios y Coworking

**XAVIER ALCALÁ NAVARRO**
Nº de colexiado: 1241
Teléfono: 670 518 226
Praza José González Dopeso, 1 - 5ºD esq.
15009 A Coruña
xalcala@iies.es
Realización de proxectos de radiocomunicacións

colexio oficial enxeñeiros de telecomunicación galicia

**www.aetg.gal**

Volver ao sumario

# Sumario



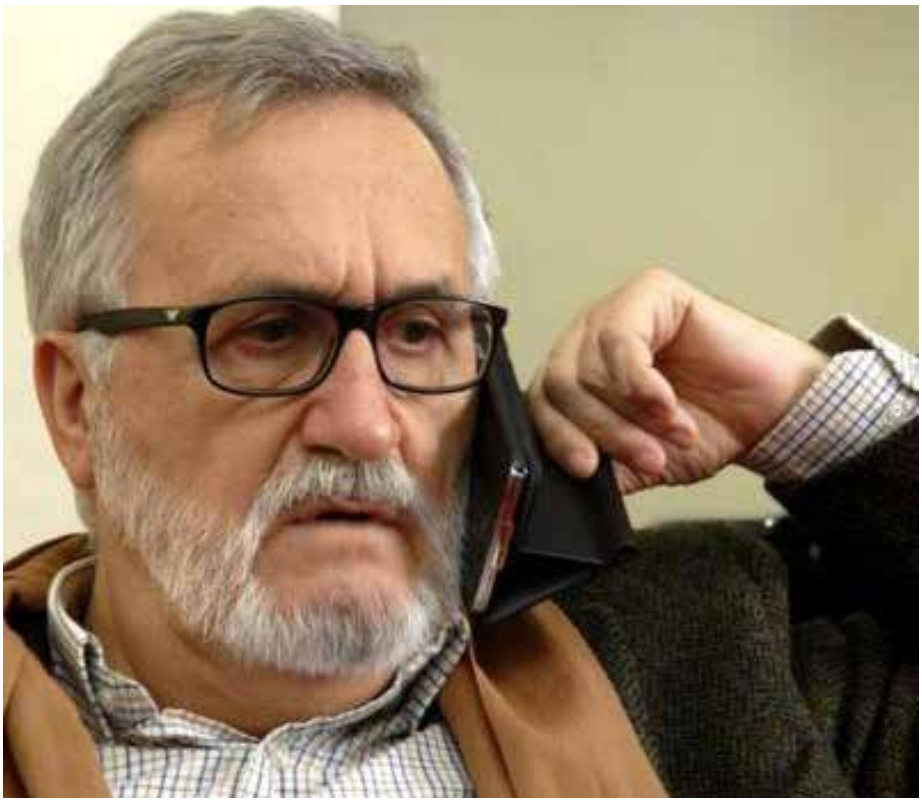
## Colaboracións:



Volver ao sumario

# Carta do director

Xavier Alcalá Navarro



Caros colegas e compañeiros:

Lembrando o meu pai, comezo cunha frase que el repetía: "de ben nacidos é sermos agradecidos".

Cando o Xulio Sánchez Agrelo me ofreceu formar parte da xunta de goberno do COETG, xa llo agradecín, porque sempre me gorentou "facer colexio" (e "facer asociación": de feito, foron décadas nas que pertencín ás xuntas, tanto ao nivel de España como de Galicia). Cando na actual xunta se propuxo pasarme a responsabilidade que abandonara o meu vello amigo Xoaquín Lameiro, acepteina gustosamente e dei as grazas.

Cadaquén de nós está nas telecomunicacións por algunha razón, ou por algún impulso non razoado. Eu estou nelas por necesidade vital, polo mesmo que me leva a fabular: para dicir que existo (e recomendo a lectura dun clásico: o artigo *Why I write* de George Orwell). Fun á universidade pensando en cousas diferentes ás telecomunicacións, como son a aeronáutica e a arquitectura; mais tiven unha revelación cando se inaugurou o novo edificio da Escola no Paraninfo de Madrid e alí vin a exposición que amosaba "unha profesión con futuro".

Nas telecomunicacións albisquei a posibilidade de que a mensaxe –o pensamento e o sentimento– chegasen moi lonxe. Mentres na miña mente bulían crónicas, letras de cancións e os primeiros relatos, estudaba como conmutaban os transistores e como radiaban as antenas. E tiven moita sorte cos meus profesores, desde don Julio de Paula y Pardal –que so lía os exames correctamente redactados– a case-compañeiros coma o Fernando Sáez Vacas, que me ensinou Informática cando iso soaba a "cousas raras da IBM".

Estou nisto por vocación, e con vocación de profesión necesaria para a sociedade asumo a responsabilidade de dirixir *A nosa rede*.

Este número da revista recolle un vasto caudal de colaboracións acerca da ciberseguridade, obxectivo que fixou a xunta de goberno como "obriga imprescindible" do noso colectivo e ao que lle dedicaramos *A Noite das Telecomunicacións do 2017*. Nas nosas páxinas maniféstanse colaboradores –individuos ou empresas– aos que poderiamos chamar no inglés que impera *stake holders* da AETG e do COETG. Os seus puntos de vista, os seus asertos, marcan liñas de actuación para un ámbito de colaboración, un ecosistema no que todos –empresas, asociación e colexio– temos espazo interactivo.

Por vontade da nosa xunta de goberno a ciberseguridade vai continuar estando presente nas páxinas de A nosa rede. Ora, a revista vai recoller máis inquedanzas do grupo de compañeiros aos que nos destes a confianza para tripularmos a nave do colectivo.

Hai agora corenta anos –si, 40, con cifra– en que eu facía de enlace entre Ferrol, Coruña, Santiago e Vigo, entre a Bazán, Fenosa, Televés e Citröen, onde traballaba a maioría dos colegas que andaban a pensar como constituírmos a delegación da AEIT en Galicia. Xa choveu desde aquela e en poucos días imos celebrar o XXV aniversario non da Delegación da AEIT senón da AETG. Tristemente non están connosco suxeitos tan teimudos coma José Arijón do Porto ou Xerardo García Campos, mais faremos un brinde ás súas memorias.

Poucas profesións mostraron en Galicia, como fixo a nosa, unha tan grande dinámica de crecemento e proxección social. Velaí o propio feito da constitución e desenvolvemento do AETG e do COETG, e a creación e desenrolo da Escola na UVigo. Somos unha realidade moi respectada, na que o sistema social pon esperanzas notorias.

Con todo, non abonda o realizado e temos retos por diante. Expoño aquí, nestas páxinas, vectores de actuación que definiu a nosa xunta e que o decano se encarga de recordarnos:

Hai novos campos de actuación para o colectivo. Véxase a ciberseguridade desde o punto de vista noso, non exclusivamente do software: a seguranza debe contar co seu soporte, cos medios de transmisión e de procesamento, coa

Volver ao sumario

mestura de *hard* e *soft* que define –interactuando– as redes. Mais non esquezamos outros coma, por non irmos máis lonxe, o dos "abellóns mecánicos".

Ninguén se asuste co que parece un novo concepto, pois é a tradución de *drones* ao galego segundo votaron maioritariamente os meus seguidores en Facebook e Twitter. Pensade en todas as aplicacións desas máquinas que so poden funcionar telemandadas e telecomunicadas. Nós temos moito que falar ao respecto. Debemos ofrecer ás administracións a nosa sabedoría (coñecemento máis experiencia) para organizar un novo mundo no que a Uber xa coloca grandes abellóns non tripulados como taxis aéreos...

Quen lle dera a Jules Verne ter sido enxeñeiro de telecomunicación na era da *web*, a arañeira universal de servidores e clientes que funciona grazas ás nosas técnicas cotiás.

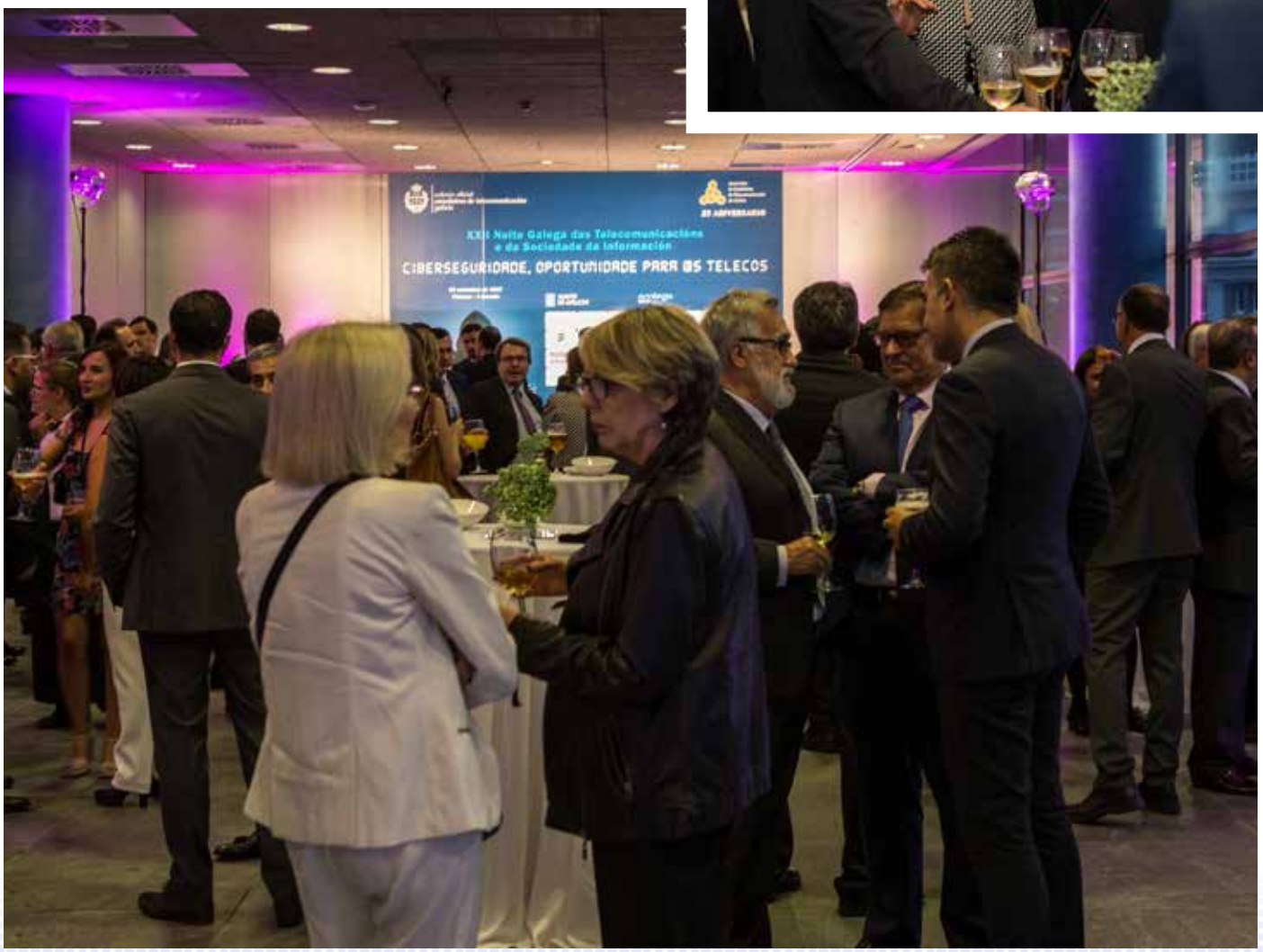
E, falando da web (que nós sabemos distinguir da Internet), quixera desde estas páxinas transmitir a inquedanza da nosa xunta a respecto da malla de relacións que cómpre establecer entre todos os compañeiros, os asociados e colexiados e os que –pola circunstancia que for– non o están.

Debemos contar a nosa historia e o noso presente como colectivo, para nós mesmos e para o resto da sociedade. Xa de inicio, a nosa responsable de comunicación, Ana Becerra, vaise encargar de que teñamos un espazo en Facebook e un perfil de Linkedin para "facermos pobo"; e –insistamos– pobo de todos os enxeñeiros de Telecomunicación de Galicia: os que exercemos neste ben querido Impaís e os que andan polo mundo, alén do Miño, das Portelas e da Pedrafita.

Neste intre a conciencia da galeguidade leva a pensar iniciativas coma a da Universidade de Vigo: tentar conectar os seus egresados que andan expatriados. Moitos dos que formamos parte das xuntas sabemos da emigración, da morriña, da saudade e da coraxe de querer facer país do Impaís. Desde aquí vaia un convite ao encontro de todos os que queiran, desde onde estiveren, participar no espazo de Facebook da AETG e n'A nosa rede, que van estar interligadas.

En fin, unha grande aperta na que todos caibades; un rogo que me manda facer o decano: que induzades os colegas a se asociaren e colexiaren; e, xa que falabamos da Diáspora Galega, un saúdo de corazón na man ao amigo Ángel Viña Castiñeiras, que impulsou a existencia dunha bela publicación en papel: *A nosa rede*.

Xavier Alcalá




Volver ao sumario

# Ciberseguridade, oportunidade para @s telecos

Crónica do evento


Baixo o lema "Ciberseguridade, oportunidade para @s telecos" celebramos a vixésimo segunda edición da Noite Galega das Telecomunicacións e da Sociedade da Información na que, como xa é tradición reunimos aos profesionais más representativos do sector TIC.

"Só desde a unión podemos avanzar e afrontar con éxito os grandes retos que se nos presentan cada día como son, entre outros, a ciberseguridade e o big data. Ou facémolo nós ou alguén o fará por nós", son as palabras de Julio Sánchez Agrelo, decano do Colexio Oficial e presidente da Asociación de Enxeñeiros de Telecomunicación de Galicia, na súa intervención na XXII Noite Galega das Telecomunicacións e da Sociedade da Información, que celebramos o venres día 29 de setembro no Palacio de Exposicións e Congresos da Coruña.

A Noite, que presidiu o presidente da Xunta, Alberto Núñez Feijoo, comezou ás oito da tarde cun networking, no que participaron uns 300 profesionais e empresarios do sector. Ás 21,30, principiou a gala -dedicada á ciberseguridade- presentada pola actriz e bailarina, Silvana Sestelo. Foi un espectáculo, tan disruptivo como orixinal, no que se conxugaron, con gran ritmo, a música, a iluminación, a danza, a proxección de vídeos, os discursos e a entrega de premios.

No seu transcurso, foron entregados os Premios Galicia das Telecomunicacións e da Sociedade da Información 2017: Paulino González Pan foi galardoado coa distinción de Enxeñeiro do Ano do COETG e a directora da Amtega, Mar Pereira como Socia de Honra da AETG. O premio Enxeñeiro Gerardo García Campos á mellor iniciativa empresarial no sector TIC concedéuselle a Situm Technologies; o premio GRADIANT á mellor tese doutoral aplicada ao sector TIC a Alejandro Ramos Soto, o Mellor Proxecto TIC con Beneficios Sociais, outorgado en colaboración coa Amtega foi para Balidea Consulting & Programming, o premio ó mellor expediente académico do Máster en Enxeñería de Telecomunicación da Universidade de Vigo para Víctor Manuel Segura Sieiro e a empresa Finsa foi galardoada co premio Acuntia á empresa galega que aposta polo desenvolvemento de infraestruturas intelixentes de telecomunicacións.

No nome dos premiados interveu o "enxeñeiro do ano", Paulino González, quen subliñou que volvendo a vista atrás, "les puedo decir que ha sido una satisfacción ejercer como teleco. Si volviera a nacer, volvería a elegir, sin lugar a dudas, esta maravillosa profesión".

González fixo referencia ao seu paso por Telettra, Airtel e Vodafone e á súa contribución ó desenvolvemento da rede de telefonía móbil de Vodafone en Galicia, que, dixo, "posibilitó la dinamización del mercado y la siempre estimulante competencia". Cunha consecuencia clara, "una mayor calidad de un servicio, que hoy es de primera necesidad".

"La infraestructura de nuestra red –engadiu Paulino González- se

***"Só desde a unión podemos avanzar e afrontar con éxito os grandes retos que se nos presentan cada día como a ciberseguridade e o big data"***

Volver ao sumario

desarrolló en igualdad de condiciones que en el resto de España, tanto en tiempo como en calidad". O que, por desgraza, dixo, "no podemos afirmar en relación con otras infraestructuras también esenciales".

O enxeñeiro do año rematou o seu breve discurso cunha referencia familiar e dedicando o premio a un "elenco de extraordinarios profesionales que me han ayudado y acompañado a lo largo de esta fantástica carrera profesional. Sin ellos nada hubiera sido posible". Por iso, "en un acto de justicia", puntualizou, "quiero compartir con todos ellos el premio que han tenido la amabilidad de concederme".

A Noite desenvolveuse logo do proceso electoral celebrado no primeiro semestre deste ano, co que se abre "unha nova etapa no Colexio e na Asociación de Enxeñeiros de Telecomunicación de Galicia". "Estamos aquí -enfatizou Julio Sánchez Agrelo- para recoller a magnífica herdanza dos equipos directivos que nos precederon e para, na medida do posible, superala e mellorala".

***"Vertebrar aos profesionais das TIC, comezando pola integración, no colexio e na asociación, de todos os enxeñeiros de telecomunicación de Galicia"***

Despois dunhas palabras de recoñecemento para o decano e presidente saínte o seu substituto sinalou que "tomamos o relevo con tanta determinación como ilusión", e fixou, como o seu principal obxectivo, "vertebrar aos profesionais das TIC, comezando pola integración, no colexio e na asociación, de todos os enxeñeiros de telecomunicación de Galicia".

Ademais, o novo decano e presidente do Colexio e da Asociación de Enxeñeiros de Telecomunicación de Galicia puxo especial énfase na "defensa da dignificación do noso traballo". E -engadiu- " reivindicaremos a nosa función como profesionais das Tecnoloxías da Información e da Comunicación. A ninguén debe molestarlle que reclamemos o que lexitimamente nos corresponde".

Antes de finalizar, Sánchez Agrelo tivo unha lembranza emocionada para Fernando Pardo, falecido hai un ano, ó que definiu "como uno de los padres fundadores de la TVG, un maestro y un magnífico divulgador de la ingeniería de telecomunicación. Una referencia a seguir, tanto en el ámbito personal como profesional".

Con este acto en Palexco e 22 anos despois da súa posta en marcha, a Noite Galega das Telecomunicacións e da Sociedade da Información pasa a ser itinerante e, nos vindeiros anos, celebrarase nas cidades máis importantes da nosa comunidade. Esta edición coincide co 25 aniversario da Asociación de Enxeñeiros de Telecomunicación de Galicia para o cal están previstos unha serie de actos conmemorativos.

Volver ao sumario

# Premios Galicia das Telecomunicacións e da Sociedade da Información 2017

**Paulino González Pan foi nomeado Enxeñeiro do Ano do COETG e Mar Pereira, directora da Amtega foi distinguida co título de Socia de Honra da AETG. Ambos compartiron galardóns, con Situm Technologies, Alejandro Ramos, Balidea Consulting & Programming, Víctor Manuel Segura e Finsa.**

O Colexio Oficial e a Asociación de Enxeñeiros de Telecomunicación de Galicia entregaron os Premios Galicia das Telecomunicacións e da Sociedade da Información 2017 no transcurso da XXII Noite Galega das Telecomunicacións, que se celebrou o 29 de setembro no Palexco da Coruña.

**O premio Enxeñeiro do Ano**, recaeu en Paulino González Pan pola súa exemplar traxectoria profesional e o seu fondo compromiso co desenvolvemento do sector das telecomunicacións no noso país e co Colexio Oficial e a Asociación de Enxeñeiros de Telecomunicación de Galicia.

**O premio Socia de Honra**, foi para Mar Pereira Álvarez, directora da Axencia para a Modernización Tecnolóxica de Galicia, pola súa contribución ó desenvolvemento das Tecnoloxías da Información e da Comunicación na nosa Comunidade e o seu compromiso co despregue da banda larga e a vertebración dixital do noso país, a implantación da Administración electrónica e a aceleración da economía dixital.

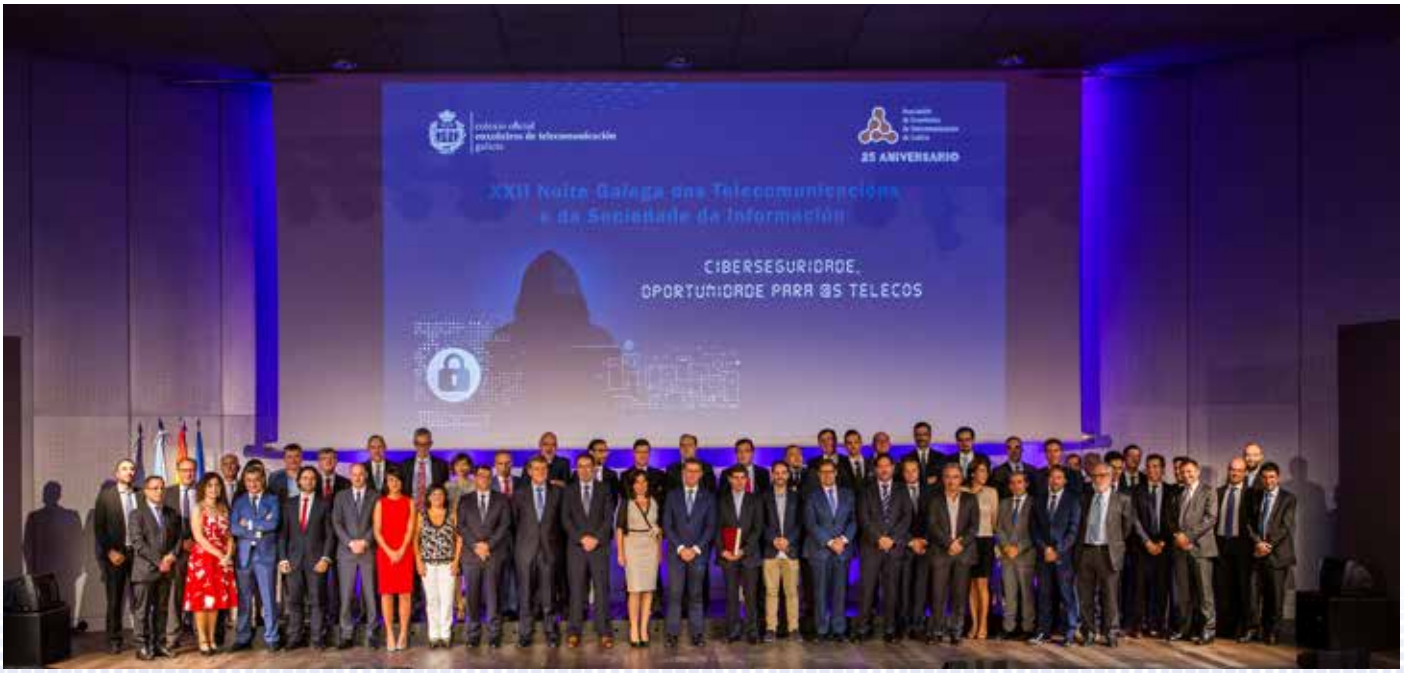
**O premio Enxeñeiro Gerardo García Campos á mellor iniciativa empresarial no sector TIC**, foi para Situm Technologies, polo desenvolvemento de produtos tecnolóxicos relacionados co posicionamento en espazos interiores, e pola súa aplicación a mercados amplos. Ademais, tívose en conta a orientación desta empresa á exportación, á I+D+i e á creación de emprego tecnolóxico.

Volver ao sumario

**O premio ó Mellor Proxecto TIC con Beneficios Sociais, outorgado en colaboración coa Amtega**, recaeu en Balidea Consulting & Programming, polo seu proxecto UnderstAID, unha plataforma de asistencia a persoas que coidan de pacientes con demencia. O xurado tivo en conta a sinxeleza coa que a ferramenta resolve esta necesidade social, e o seu potencial para chegar a un gran número de usuarios.

**O premio ó Mellor expediente académico do Máster en Enxeñería de Telecomunicación da Universidade de Vigo**, foi para Víctor Manuel Segura Sieiro.

**O premio GRADIANT á mellor tese doutoral aplicada ó sector TIC**, recaeu en Alejandro Ramos Soto, por Aplicación de conxuntos difusos en sistemas de date-to-text. O xurado salienta o innovador desta técnica, empregada para xerar escritos en linguaxe natural a partir de datos, xunto co seu alto impacto en publicacións de referencia. A sanidade, a meteoroloxía, ou a educación son algúns dos ámbitos nos que este traballo xa ten demostrado a súa utilidade.




Volver ao sumario

# Empresas galegas na vangarda da era dixital

## A madeireira FINSA galardoada co premio Acuntia 2017

Cada ano o Colexio Oficial e a Asociación de Enxeñeiros de Telecomunicación de Galicia convoca os Premios Galicia das Telecomunicacións e da Sociedade da Información. Estes galardóns constitúen unha excelente plataforma para a promoción e proxección das empresas e profesionais galegos e dos produtos e servizos que se están a desenvolver no sector TIC en Galicia. Un destes galardóns é o premio Acuntia, que recoñece ás empresas galegas que apostan polo desenvolvemento de infraestruturas intelixentes de telecomunicacións.

Promovido polo COETG e a AETG e patrocinado pola entidade que lle dá nome, o premio Acuntia destaca ás empresas de orixe galego que apostan, como parte da filosofía empresarial, polo desenvolvemento de infraestruturas intelixentes de telecomunicacións nos seus centros de produción e na súa actividade. Este galardón, que acadou este ano a súa cuarta edición, outorgase con carácter anual, grazas a empresa Acuntia, patrocinadora tamén da Noite Galega das Telecomunicacións e cunha importante presenza no sector das TIC nos últimos 25 anos a nivel nacional.

Este ano a compañía Financiera Maderera S.A. -FINSA- foi a galardoada co premio Acuntia 2017 á empresa galega que aposta polo desenvolvemento de infraestruturas intelixentes de telecomunicacións, na vixésimo segunda edición da Noite Galega das Telecomunicacións e da Sociedade da Información celebrada o pasado mes de setembro en A Coruña e organizada polo Colexio Oficial e a Asociación de Enxeñeiros de Telecomunicación de Galicia. Os motivos determinantes desta distinción definíronse principalmente, segundo o xurado, pola evolución da compañía cara a produtos alto valor engadido dentro da cadea de transformación da madeira e pola súa expansión nacional e internacional, ás que contribuíu sen dúbida a renovación tecnolóxica da súa infraestrutura TIC nas súas oficinas e centros de produción.

Nas súas plantas de produción FINSA implementou unha plataforma de telecomunicación co obxectivo de consolidar a información de cara a incorporar intelixencia artificial aos seus procesos. En 2011, a compañía converteuse en 2011 no primeiro fabricante de madeira técnica da Península Ibérica o que garante unha produción procedente de bosques xestionados de forma sostible. Fundada en 1931 conta con centros de produción en España, Francia e Portugal cunha rede loxística que facilita a súa presenza en máis de 80 países.

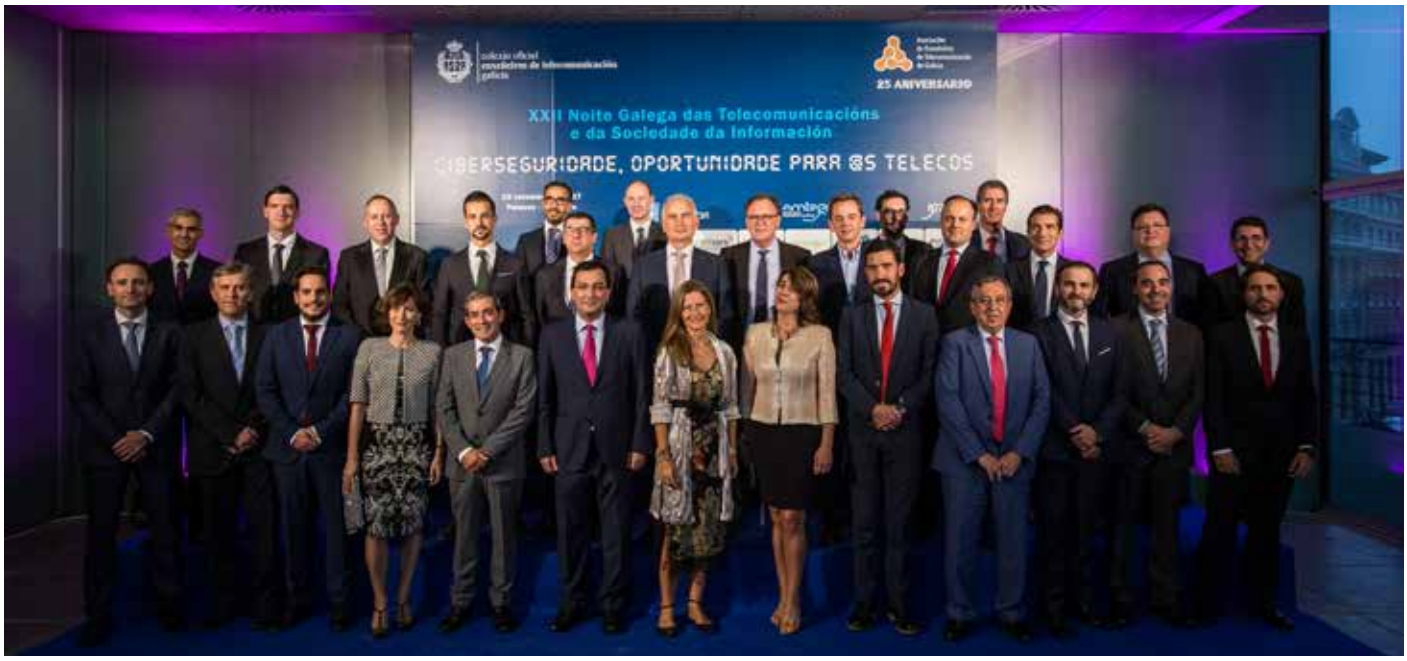
*Germán Viso Rodríguez, Director Económico Financeiro de Finsa*

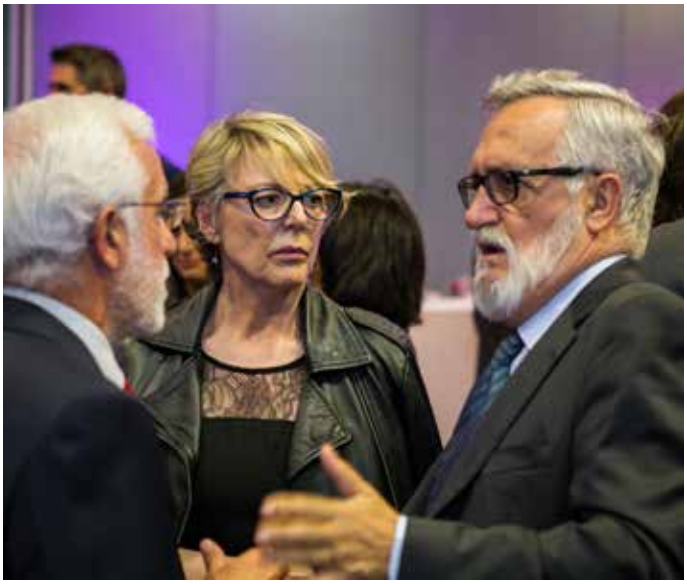

*Javier García Pazos, Director TI de Finsa asinando no libro de firmas do Colexio*


*Emilio Cabañas, Director xeral de Acuntia*

Volver ao sumario

# Galería do evento

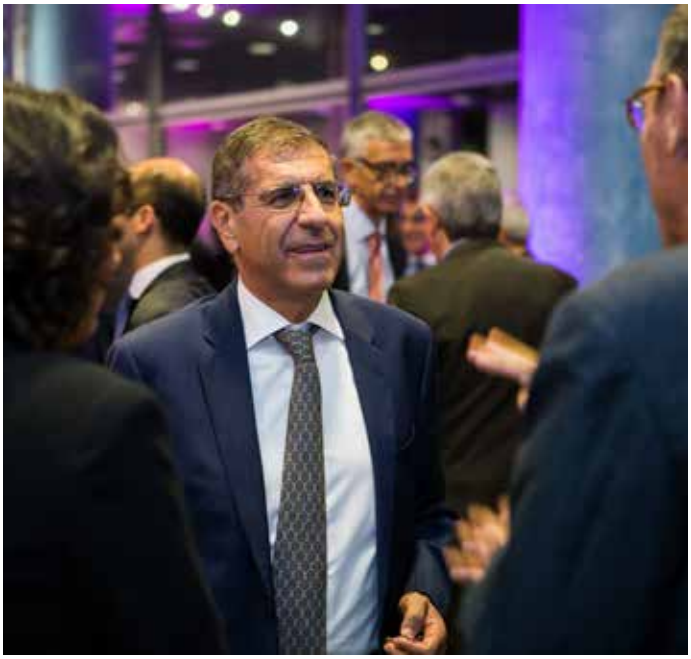


Volver ao sumario

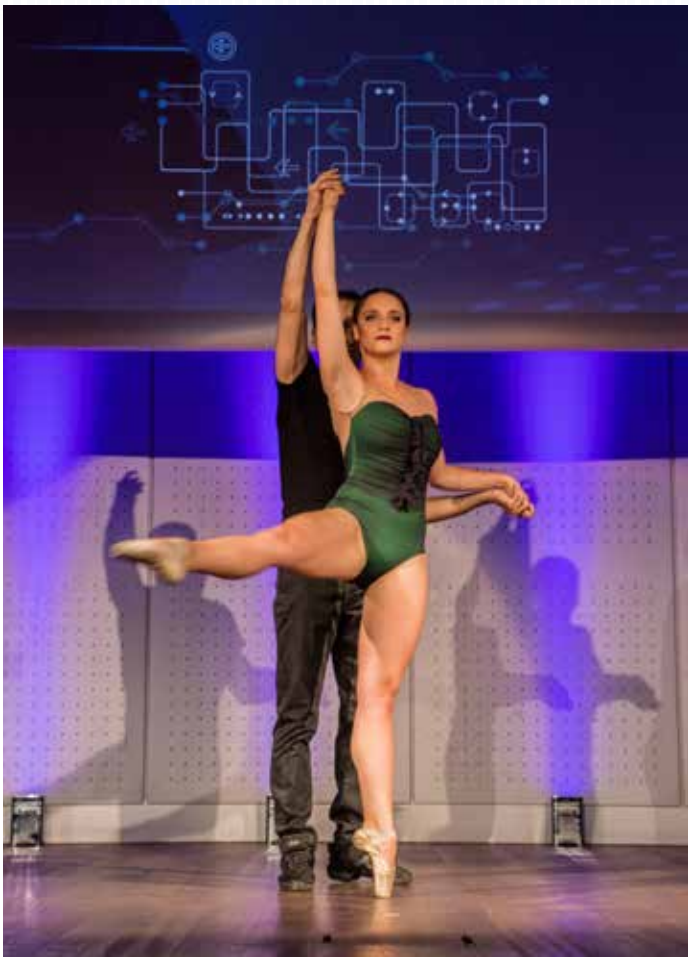
# Galería do evento


Volver ao sumario



Volver ao sumario

# Galería do evento



Volver ao sumario

# Galería do evento


Volver ao sumario

# Galería do evento


Volver ao sumario

# A Ciberseguridade, elemento prioritario dun mundo dixital

Mar Pereira
Directora da Amtega

XUNTA DE GALICIA

amtega
Axencia para a Modernización Tecnolóxica

O 2017 pasará á historia da ciberseguridade como o ano no que se materializou a ameaza dun ciberataque global. Como unha lente de aumento o virus WannaCry deu visibilidade á escala mundial ao momento no que os ciberdelicuentes conseguen o seu obxectivo máis ansiado, o intre no que atopan a vulnerabilidade que lles permite minar as infraestruturas dixitais das entidades.

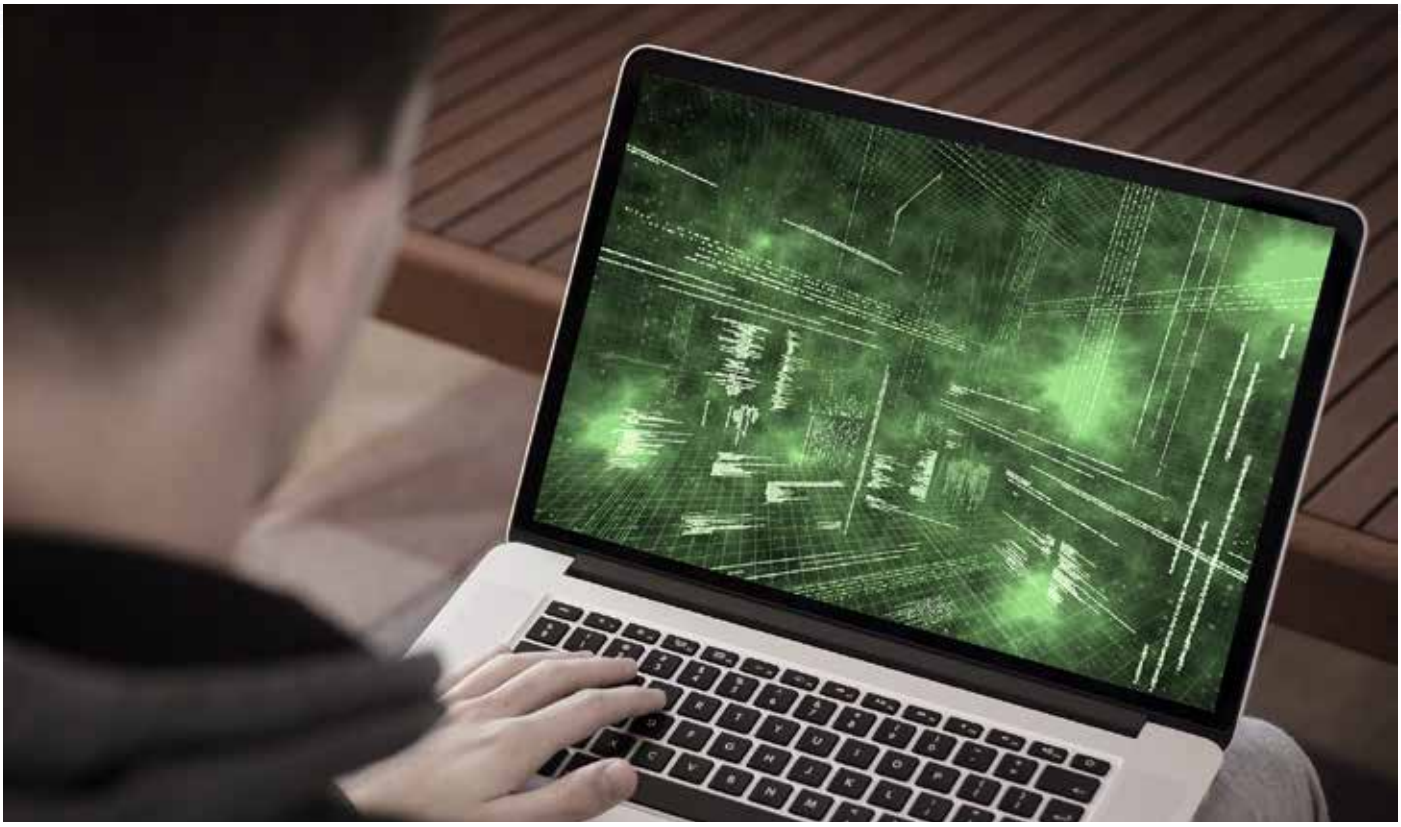
A potencia de WannaCry tivo consecuencias de diferente calado para as empresas e administracións públicas dos 150 países afectados pero evidenciou que non hai unha blindaxe 100% efectiva ante a ciberdelincuencia. A mellor defensa é estar preparados para poder detectar os posibles incidentes, acurtar os tempos de resposta ao máximo posible, minimizar o seu impacto e a desconfianza dos usuarios. Esta é a batalla diaria que empresas e administracións públicas mantemos para garantir a seguridade dos nosas infraestruturas dixitais.

***"Os ciberataques poñen en risco un dos activos máis importantes para empresas e administracións, os datos"***

Os ciberataques poñen en risco un dos activos máis importantes para empresas e administracións, os datos. Tanto o sector público como o sector privado estamos nun camiño sen retorno cara unha atención integramente dixital, na que a información é a pedra angular no deseño de servizos personalizados. Custodiamos información sensible, que debemos protexer coas máximas garantías e por iso a ciberseguridade é un elemento chave de seguridade nacional e internacional, no entran en xogo aspectos tecnolóxicos pero tamén xurídicos e que require colaboración e suma de esforzos.

A entrada en vigor en maio de 2018 do novo Regulamento Europeo de Protección de Datos homoxeneizará a normativa neste ámbito en Europa. Esta nova lei é a máis esixente nesta materia e incorpora novos dereitos parza os cidadáns como o dereito ao esquecemento, o consentimento expreso ou a portabilidade dos datos e implica un maior compromiso das organizacións públicas e privadas coa protección de datos e unha forma diferente de xestionalos.

Volver ao sumario



Estamos en plena conta atrás para adaptármonos ao este novo marco normativo. Un proceso complexo que na Administración autonómica enmarcamos no Plan Director de Seguridade TIC da Amtega. Nos dous últimos anos as medidas deste Plan incrementaron a nosa capacidade de prevención, detección e reposta ante incidentes de seguridade e facilitaron unha maior colaboración cos corpos e forzas de seguridade do Estado, achegando información de valor para axudar na investigación de posibles de delitos relacionados co ciberespazo. O Plan incide ademais na concienciación dos empregados públicos, cuxa implicación é fundamental no proceso transformación dixital da Administración. A xestión da ciberseguridade tamén tivo impacto a nivel organizativo coa constitución de órganos colexiados con participación de tódalas consellerías da Xunta de Galicia, a Asesoría Xurídica e Amtega, xa que a seguridade da información non é un aspecto unicamente técnico e é necesario elevar esta cuestión a niveis directivos das organización.

As liñas de actuación deste Plan Director reforzaranse coa Lei de Administración Dixital de Galicia (LEDIXGA), actualmente en proceso de elaboración, e coa que buscamos prestar un servizo personalizado e proactivo, no que serán esenciais técnicas de Big Data así como a compartición de información entre as administracións.

Buscamos ofrecer máis e mellores servizos dixitais pero tamén dinamizar o seu uso, xerando un clima de confianza, que require da colaboración conxunta de gobernos, corpos e forzas de seguridade e sector tecnolóxico. Informar e concienciar á sociedade sobre os posibles riscos e as importantes vantaxes da sociedade dixital é outro dos aspectos nos que non debemos baixar a garda.

O cibercrime é unha tendencia que crecerá de xeito exponencial nos vindeiros anos e non só cuantitativamente senón tamén no nivel de sofisticación. Ambos factores están a xerar unha demanda importante de profesionais cun alto nivel de especialización no campo da ciberseguridade. O novo Regulamento europeo establece entre as súas obrigas a de contar coa figura do delegado de protección de datos, un novo perfil profesional que precisará de formación específica. A adaptación dos estudos á demanda do mercado é un reto conxunto que administracións, universidades e sector tecnolóxico non podemos perder de vista.

A ciberseguridade é xa inherente ao funcionamento de empresas e institucións dun mundo dixital e ten que ser unha prioridade para previr, perseguir e neutralizar ofensivas que poden poñer en risco sectores estratéxicos da economía e da seguridade nacionais. A creación dun clima de seguridade e confianza dixital que reforce a protección dos organismos públicos e privados é vital para estimular a implicación dos cidadáns nunha contorna dixital e para acadar o pleno desenvolvemento dunha sociedade dixital na que os incidentes de seguridade son cada vez máis frecuentes e complexos.

***"O novo Regulamento europeo establece entre as súas obrigas a de contar coa figura do delegado de protección de datos, un novo perfil profesional que precisará de formación específica"***

Volver ao sumario

# A importancia do inadvertido na ciberseguridade

Javier Jurado
Gerente de Desarrollo de Negocio e Ingeniería Preventa de Acuntia

Ante o desafío das ameazas actuais á seguridade nas TIC, adoitamos abarrotarnos de palabrexos técnicos, últimas tendencias, novas vulnerabilidades e discusións sobre a súa motivación (activista, política e sobre todo económica). Pero en ocasións, convén non perder de vista que case todo o concernente á ciberseguridade pasa por advertir cousas que damos por suposto ou nas que non reparamos. Evidentemente, na inmensa maioría dos casos as vulnerabilidades explotadas eran inadvertidas. Ou, como mínimo, infravaloradas. Pero esta vez gustaríame levar a reflexión un pouco máis aló da importancia dos servizos para a análise de vulnerabilidades ou o hacking ético, ou das solucións para a remediación e protección destas vulnerabilidades distraídas.

## O protagonismo humano

Por exemplo hai unha perogrullada en ocasións esquecida e é que o núcleo da seguridade son as persoas, sexan civís, militares, cidadáns, empregados, pacientes, clientes, empresarios ou accionistas. Esta obviedade forma parte dese tipo de "principios de deseño" que se esquecen ou se dan por sentado e ás veces acaban sendo traizoados cando se establecen para o TIC as políticas públicas, os proxectos de investigación, as liñas de desenvolvemento tecnolóxico, os plans directores corporativos, a gobernación dos servizos ou o desenvolvemento de novos modelos de negocio.

Ao ser humano converxe necesariamente a tecnoloxía, sempre con tendencia antropomorfa. Os dispositivos de acceso converxen porque o ser humano segue contando co mesmo par de petos que hai séculos. Ademais, para acompañar ao nómade posmoderno, estes dispositivos son definitivamente inalámbricos, xa que naturalmente o home perdeu co seu cordón umbilical o último enchufe. Do mesmo xeito, as plataformas e solucións de seguridade perseguen o comportamento humano, perfilándoo, conténdoo ata o endpoint, vixiando a súa pegada dixital,... Esta procura do extremo a extremo non ten senón ás persoas como centro da súa atención, ben sexa como obxectivos a protexer ou como potenciais atacantes.

Pero esquecer que o erro humano é a causa, aproximadamente, do 25% das brechas de seguridade, e que a intencionalidade maliciosa atópase tras a maioría do resto de brechas (cos seus particulares intereses e motivacións) pode ser un problema de miopía tecnolóxica, atolondrada entre o extremo do investimento desnortado e o extremo da austeridade suicida. Unha xestión eficiente e eficaz dos recursos é imprescindible. A psicoloxía, a socioloxía, a política ou mesmo a antropoloxía son disciplinas que ben poden contribuír a enmarcar e racionalizar esta loita global pola ciberseguridade, que require ser comprendida na súa totalidade.

Decía Ortega y Gasset: Vean, pues, los ingenieros que para ser ingeniero no basta con ser ingeniero. Para facer fronte ao reto da ciberseguridade actual, é preciso ir máis aló e advertir as facetas esquecidas das persoas completas. E por tanto, considerar e ser homes completos, integrais, ou o que é o mesmo, íntegros. A dimensión ética en defensa da ciberseguridade é un factor habitualmente menosprezado, por ser aparentemente irrelevante. Nin atacantes nin atacados parecen compelidos por ela. Pero sen o seu fundamento, a súa concienciación, a súa consideración é imposible seguir pondo portas ao campo no que se expoñen recurrentemente as nosas vulnerabilidades. Sempre haberá "malos". Pero por que o son e que poderiamos facer para que fosen menos, e que estamos a facer para gañarnos nosos merecidos "inimigos" son preguntas que non hai que evadir. Unha responsabilidade social corporativa auténtica -máis aló da mercadotecnia social- das empresas ou unhas políticas públicas democraticamente orientadas poderían axudar enormemente ás nosas organizacións neste ámbito da ciberseguridade.

## A ciberseguridade como ausencia

***"A psicoloxía, a socioloxía, a política ou mesmo a antropoloxía son disciplinas que ben poden contribuír a enmarcar e racionalizar esta loita global pola ciberseguridade, que require ser comprendida na súa totalidade"***

Volver ao sumario


***"A nosa seguridade, como ben inadvertido, está permanentemente en xogo aínda que non o saibamos"***

Como dicía, a seguridade está sempre en xogo, en loita -agón, e de aí, en ocasións mesmo, en agonía. En loita porque para garantila hai que pelexala. E ignoralo é en si mesmo perigoso. A seguridade, pola súa propia natureza, é evasiva, negativa, en tanto que resulta un intanxible que se define habitualmente pola carencia doutras realidades. Seguridade é inexistencia de ameaza, ausencia de violencia, falta de usurpación, carencia de engano. A seguridade defínese como a ausencia do outro, como esa normalidade na que un desexa poder vivir. E por tanto, adoita pasar inadvertida... ata que desaparece. Os orzamentos públicos e privados en materia de seguridade sempre parecen excesivos. Ata que, de súpeto un día, móstranse lamentablemente imprescindibles.

E se a este carácter negativo da seguridade súmase o modo en que imos asimilando a presenza das TIC, a importancia do inadvertido cobra aínda máis valor. Porque é obvio xa que a tecnoloxía penetrou as nosas vidas ata volverse invisible, transparente, camuflada tal e como sucede coa luz ou a auga quente, sen as cales poucos saberían sobrevivir a pesar de non apreciala no seu día a día. A nosa seguridade, como ben inadvertido, está permanentemente en xogo aínda que non o saibamos.

Pero tampouco pode obviarse que a seguridade estivo sempre irmandada  con outro valor humano, que tamén comparte o seu carácter negativo e inadvertido, pero que en moitas ocasións contrapónselle: falo da liberdade. Historicamente, toda a loita liberal enfrontouse a un Estado coercitivo que se lexitimaba na seguridade que nos proporciona. A literatura política respecto diso é interminable. Como con acerto definía I. Berlin, a liberdade negativa (como ausencia de coerción) entrou en conflito moitas veces coa liberdade positiva (aquela que nos facilita os recursos e medios para poder elixir, por exemplo sería o feito de sentirnos seguros). Como é ben sabido, normalmente, canto máis seguros estamos, menos marxe de manobra temos.

O crecemento exponencial dos ciberataques que vivimos nos nosos tempos, no contexto dun mundo globalizado polas TIC e axitado por unha xeopolítica multipolar e un terrorismo que tamén deu o salto á tecnoloxía, contribúe a acrecentar unha onda que, sobre todo desde o 11S, leva pondo en xogo a nosa liberdade e os nosos dereitos subrepticiamente. Snowden ou Manning foron fitos mediáticos desta política, lexitimada na seguridade, e que a pesar de promocionarse como perseguidora desa "liberdade duradeira", segue erosionando inadvertidamente os nosos dereitos. O excesivo celo pola seguridade pode facilmente dexenerar, ao servizo de intereses espurios, en prácticas abusivas que, moitas veces, aprovéitanse de nós tras inxectarnos medos infundados.

Este dilema, necesitado dun equilibrio entre liberdade e seguridade, tamén se dá nas nosas organizacións: a excesiva flexibilidade e axilidade ao servizo do negocio ou da entidade pública poden comprometer severamente a seguridade. En sentido contrario, unha excesiva preocupación pola seguridade lastra a nosa capacidade operativa e funcional, reducindo a nosa competitividade e a calidade do noso servizo e/ou produto. Todo exercicio que nos axude a facer visibles as causas e circunstancias que afectan o escenario da ciberseguridade seranos útil para preservala con intelixencia.

Volver ao sumario

# Un futuro ilusionante

Sonia Lois García
CEO de Coremain


Coremain cumpriu o ano pasado 25 anos sendo unha referencia en España no ámbito da consultoría e o desenvolvemento de solucións TIC para empresas e institucións. Foi un aniversario marcado pola integración da empresa no grupo Kiom, do que forman parte firmas de referencia como Sivsa ou Autronic, o que está a servir para dar un novo impulso ao desenvolvemento da empresa e potenciar as súas fortalezas, apoiándonos na experiencia compartida en todos estes anos.

Desde a nosa sede en Galicia, Coremain acumulou un merecido prestixio en toda España e en moitos ámbitos e sectores estratéxicos da nosa economía. En telecomunicacións, Coremain é na actualidade provedor tecnolóxico homologado no tres principais operadores do mercado nacional. Neste ámbito, traballamos cos nosos clientes en proxectos de implantación e integración de sistemas propios e de terceiros, no ámbito dos sistemas de apoio ao negocio (BSS) como á operación (OSS), mediante contratación directa ou en estreita colaboración cos principais fabricantes e integradores a nivel internacional. É nesta área onde tamén se está desenvolvendo na actualidade un proxecto para a virtualización de máis de 8.000 postos de traballo, no cal todas as aplicacións, contidos e datos quedan protexidos no propio centro de datos, non nos dispositivos utilizados polos usuarios, achegando as máximas garantías e avances en termos de ciberseguridade, conformidade do usuario ou acceso remoto desde calquera lugar.

***"Na área de Business Process Outsourcing (BPO), Coremain apostou por un equipo altamente especializado e cun modelo de servizo de soporte externalizado"***

Na área de Business Process Outsourcing (BPO), Coremain apostou por un equipo altamente especializado e cun modelo de servizo de soporte externalizado, co que non só xestionamos xa máis dun millón de incidencias técnicas, senón que adquirimos unha experiencia e un coñecemento fundamentais, a través dos cales puidemos deseñar e pór en marcha ferramentas propias de automatización e optimización, utilizadas a día de hoxe por algúns dos principais operadores de telefonía do noso país. Con iso, ademais, conseguimos incrementar

Volver ao sumario

o grao de satisfacción dos nosos clientes e asegurar os maiores estándares de calidade.

Do mesmo xeito, a implementación de ferramentas TIC no sector sanitario, sector que destaca pola enorme complexidade dos procesos asistenciais e sanitarios e a especial sensibilidade da información e os datos manexados nas súas contornas, converteuse noutro dos eixos principais para a compañía. A nosa experiencia no ámbito da sanidade, e a aplicación de innovadoras solucións tecnolóxicas, permitiron mellorar a eficiencia dos procesos asistenciais nos centros sanitarios públicos, e optimizar a xestión dos recursos. Tanto é así que na actualidade, Coremain, cun equipo de máis de cen persoas traballando especificamente nesa área, desenvolve servizos de soporte e xestión evolutiva dos sistemas informáticos utilizados polos profesionais do sistema sanitario público de Galicia dentro dos seus procedementos asistenciais, garantindo o seu correcto funcionamento as 24 horas e os 365 días do ano. Neste ámbito, Coremain apostou polo investimento en innovación, participando recentemente no Plan de Innovación Hospital 2050, impulsado pola Xunta de Galicia e a consellería de Sanidade e cofinanciado polos Fondos FEDER, para desenvolver proxectos que melloren a calidade asistencial dos hospitais públicos galegos, enfocando un novo modelo centrado no paciente.

Ademais, no caso dos produtos e sistemas que desenvolvemos para o ámbito sanitario, garantimos sempre que están construídos tendo presente, como requisito de primeiro nivel, as máximas medidas de seguridade en canto á xestión da información, garantindo a autenticidade, confidencialidade, integridade e dispoñibilidade desa información no seu tratamento, procesado e almacenamento.

Por outra banda, nos servizos que prestamos aos nosos clientes do ámbito sanitario achegamos como valor engadido un plan de seguridade da información baseado no normativa ISO 27000, na que nos atopamos

***"Coa integración en Kiom, a nosa empresa ábrese a un futuro aínda máis ambicioso, optando a novos sectores e áreas de traballo"***

certificados, e que propón as políticas de seguridade e liñas de actuación que se aplican sobre cada un dos sistemas a protexer, sobre a seguridade ligada aos recursos humanos (acordos asinados de confidencialidade para todos e cada un dos membros dos equipos que compoñen os servizos), medidas de seguridade física e ambiental (acceso controlado aos equipos e CPD), medidas e procedementos de copias de seguridade, actuacións ante código malicioso, control e uso de correo electrónico, monitorización da rede de comunicacións, rexistro de acceso á información, auditoría de eventos, detección e corrección de vulnerabilidades de seguridade da información, xestión de usuarios e plans de continuidade con simulacros de recuperación ante desastres.

En materia de Educación, Coremain traballou, entre outros, na mellora e evolución do sistema de xestión de persoal docente da Consellería de Educación do Goberno de Cantabria, adaptándoo e dando soporte de maneira continuada, un proxecto sólido que habemos ido mellorando grazas aos máis de dez anos de colaboración con esta institución.

En definitiva, pemes, administracións públicas e a industria en xeral foron coñecedores, durante os últimos 25 anos, do traballo innovador de Coremain, por iso agora, coa integración en Kiom, a nosa empresa ábrese a un futuro aínda máis ambicioso, optando a novos sectores e áreas de traballo, complementándonos coas demais empresas do grupo e reforzándonos como unha das empresas líderes en desenvolvementos Tics. en España. 25 anos despois, o futuro de Coremain preséntase máis ilusionante que nunca.

Volver ao sumario

# Como pode aumentar a concienciación sobre as mellores prácticas de seguridade cibernética na súa organización

Nuria Andrés
Network Integration & Security LoB Manager de Dimension Data

Dado o incremento de ataques avanzados de ciberseguridade nos últimos anos, non é ningunha sorpresa que a industria estea a adoptar un enfoque máis proactivo para protexer os datos.

O noso *2017 Global Threat Intelligence Report* revelou que o ano pasado houbo un 11% de melloría interanual no número de organizacións que evolucionaron activamente a súa preparación para a resposta ante ataques. Con todo, a investigación tamén revelou que o 68% das organizacións non teñen un plan formal de resposta a ataques.

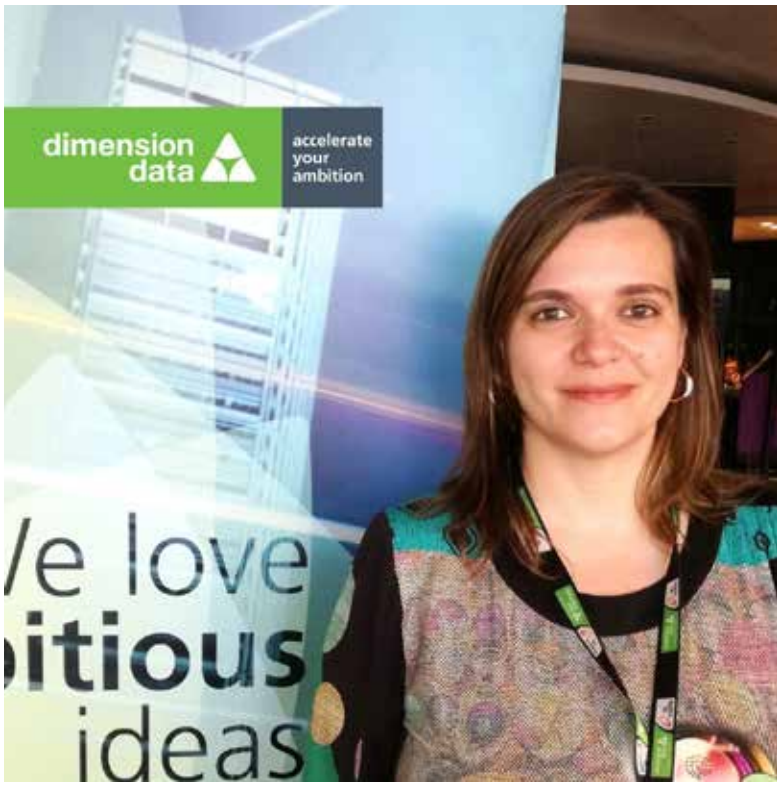
Como pode a súa organización converterse nunha desas empresas que evolucionan activamente a súa resposta ao panorama actual da ciberseguridade? Aquí non hai unha única fórmula para o éxito. Con todo, se está listo para actuar en prol da seguridade cibernética, de seguido, proporcionarémoslle uns pasos esenciais que pode seguir para lograr este obxectivo.

Para obter máis información, o noso novo libro, *Ransomware: The Pervasive Business Disruptor*, de Frost & Sullivan, describe os factores e impactos das ameazas cibernéticas máis importantes aos que se enfronta a súa organización. Proporciona un resumo das últimas investigacións sobre ransomware e ofrece orientación sobre como limitar ese risco. Animámoslle a descargar a súa copia gratuíta do informe hoxe.

**Sexa un catalizador do cambio**

Como destaca o noso informe, o ransomware é agora a maior ameaza cibernética que afronta a industria. Unha vez activado, o ransomware pode "bloquear" aos usuarios dos arquivos e cartafoles comerciais ata que se pague o rescate ao atacante. Esta forma de ataque é moi eficaz e está a crecer en popularidade. Os beneficios para os hackers son claros: este é un negocio lucrativo e por iso os ciberdelincuentes detrás dos ataques de ransomware están constantemente desenvolvendo novos métodos para aproveitar as debilidades na infraestrutura das súas vítimas.

Que pode facer a súa organización para minimizar os riscos de ransomware e outras formas de hacking? Aínda



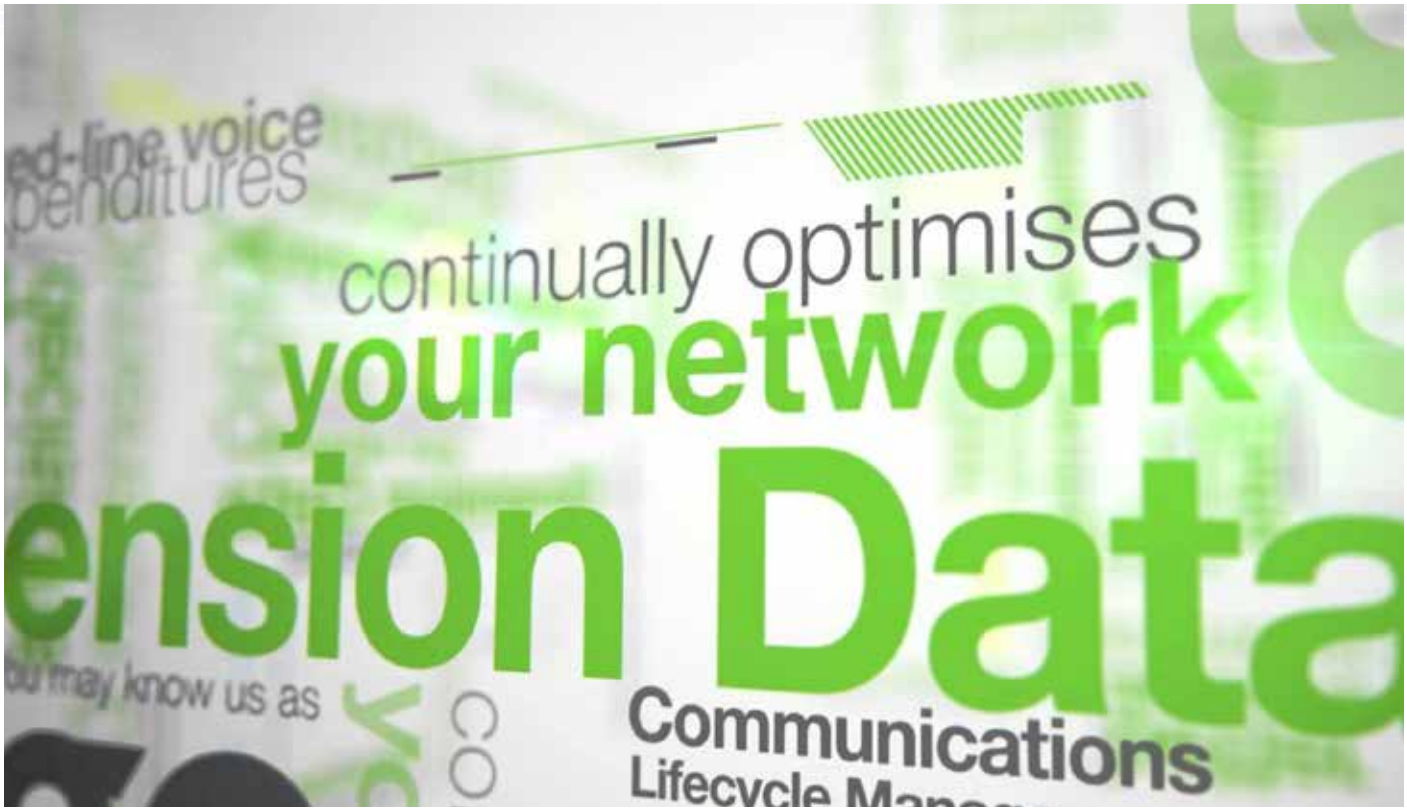

***"O 77% dos obxectivos de ransomware atópanse principalmente en catro industrias: servizos empresariais e profesionais, goberno, sanidade e venda polo miúdo"***

que o éxito a longo prazo implicará unha estratexia eficaz para adaptar a forma en que a súa organización se ocupa da ameaza, hai varios pasos que pode seguir de inmediato para empezar a limitar os riscos, iniciar conversacións na súa organización e ser un catalizador do cambio.

**1. Investigue que ameaza ao seu negocio**

Ter unha comprensión realista dos riscos que enfronta a súa organización é unha parte esencial da prevención de

Volver ao sumario




***"Para que calquera iniciativa de seguridade cibernética sexa exitosa, é esencial incluír o tema na axenda dos líderes da súa organización"***

ataques. Aínda que cada empresa enfróntase á ameaza de ransomware, é importante entender que certos sectores son atacados máis a miúdo. A nosa investigación revelou que o 77% dos obxectivos de ransomware atópanse principalmente en catro industrias: servizos empresariais e profesionais, goberno, sanidade e venda polo miúdo.

**2. Entenda o "factor humano"**

Tamén é importante entender como é máis probable que a súa organización sexa atacada. A nosa investigación reafirma a idea xeneralizada de que os seres humanos son o punto máis débil nas defensas da ciberseguridade dunha empresa. Os ataques de phishing, enxeñería social e ransomware son case todos como consecuencia de erros dos empregados individuais.

**3. Obteña o apoio executivo**

Para que calquera iniciativa de seguridade cibernética sexa exitosa, é esencial incluír o tema na axenda dos líderes da súa organización. Mentres que calquera CEO responsable entenderá a importancia da ciberseguridade, moitos o verán como un problema de TI, e poden ser remisos a tratar isto como unha das iniciativas a longo prazo do negocio.

Sen a aceptación dos líderes da organización, será difícil conseguir que a súa empresa estea ao nivel do novo panorama da ciberseguridade. A seguridade hoxe en día é omnipresente, e xa non se trata só de instalar fráxiles devasas. Esta mensaxe debe ser transmitido aos líderes da súa organización:

- Trate o tema co seu xefe de liña e tente elevalo ás reunións do comité executivo.
- Compile as últimas investigacións (descargue o noso informe técnico e infografía) e subminístreas aos líderes empresariais.
- Reúna un plan integral para o seu negocio.

Por último, ao "promover" a importancia de actualizar a súa estratexia de seguridade cibernética, faga fincapé nos custos dos períodos de inactividade, non nos rescates. Para os negocios máis grandes, un rescate de 1.000€ pode non sentirse como un desembolso enorme. Con todo, no contexto dun día (ou máis) de traballo perdido, os custos poderían chegar ás decenas ou mesmo centos de miles de euros.

**Seguintes pasos**

Os riscos son menos predicibles que antes e os atacantes están a desenvolver formas máis sofisticadas de sabotear as súas defensas. Para adaptarse a este cambio, necesitará un enfoque maduro e completo da ciberseguridade. Unha vez que teña completo apoio dos líderes da súa empresa, será capaz de desenvolver unha estratexia de seguridade con enfoque global.

Para obter máis información sobre as ameazas ás que se enfronta a súa organización, descargue o noso informe ou póñase en contacto cos nosos expertos.

Volver ao sumario

# Cidades intelixentes, coches autónomos, portos dixitais, son seguros?

Rafael Ave
Director área de Transformación Digital e Ciberseguridade de Emetel

A ciberseguridade é un habilitador necesario para a transformación dixital.

Drivers como a IoT, as novas capacidades de comunicacións, a hiperconectividade o Big Data e/ou a computación na nube, levaron a capacidade das empresas de producir información dixital dos seus procesos a un nivel impensable hai uns anos.

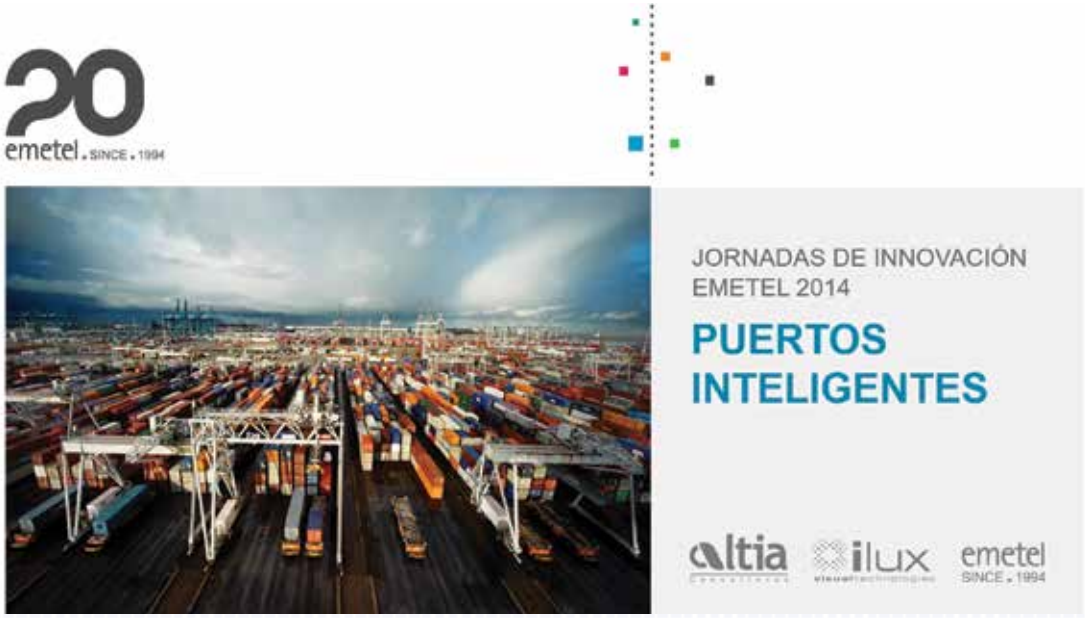
Coa evolución das técnicas de automatización de procesos, integración de sistemas e análises destes datos, a Transformación Dixital é un feito e converteuse nunha novo paradigma imparable. Un claro exemplo desta transformación ou dixitalización podémola ver nos portos.

En marzo do 2014, desde Emetel promovemos unha xornada cos portos do noroeste para empezar a traballar no concepto de "Porto Intelixente". O obxectivo era promover un novo modelo de porto no que todos os elementos estivesen integrados entre si e aliñados coas operacións e servizos portuarios. Este novo modelo implicaba conectar aos axentes portuarios (amarradores, prácticos, remolcadores, terminais, etc.) pero tamén os sistemas físicos (guindastres, radares, barcos, cámaras, controis de accesos, etc.), sistemas de información (facturación, xestión de dominio público, DUE, GIS, etc.) e administracións (Aduanas, Facenda, Portos do estado, etc.). O novo modelo creaba un porto hiperconectado.

***"Se algo é real, é que en pouco tempo todas as empresas serán tecnolóxicas, sexa cal for o seu ámbito de actividade"***

Na actualidade, o sector xa non se expón outra opción, e desde Emetel, estamos a desenvolver este modelo con varios deles: Vigo, Coruña, Avilés, Cartaxena e Cádiz, principalmente.

Neste porto dixital hiperconectado a seguridade pasa a ser un elemento crucial para minimizar os riscos operacionais garantindo operacións e servizos portuarios. Calquera ciberincidente podería manipular a información do porto, paralizar a actividade do mesmo ou,




Volver ao sumario

mesmo, pór en risco vidas humanas. Os seus efectos menoscabarían a reputación de calquera porto que podería provocar o cesamento da súa actividade.

Por iso debemos construír portos dixitalmente seguros, xestionar estes riscos en tres liñas de actuación:

• Persoas. O obxectivo é capacitar ao persoal e para iso debemos planificar desde o principio do proceso actividades de información, sensibilización e formación. A comunicación é gran aliado para xestionar o cambio, a capacitación do persoal un elemento indispensable para o éxito.

• Procesos. Aplicar as boas prácticas de modelos como o ISO 27k, ENS, LPIC, etc. Non só serve para eliminar o risco legal. Ben aplicadas permiten adoptar sistemas de xestión da seguridade da información que achegan boas prácticas a ter en conta.

• Servizos. Un conxunto ben planificado de servizos de seguridade xestionada son claves. Estes servizos van desde as medidas de prevención e detección de ciberincidentes, ata as capacidades de resolución dos mesmos.

Un consello: empeza por un Plan Director de Seguridade, esta ferramenta permitirache ter a folla de ruta que a túa organización necesita.

Pero esta revolución non é exclusiva das empresas ou as administracións públicas, cada vez máis se achega a todos nós na nosa vida cotiá. A manipulación maliciosa dos numerosos sensores dos vehículos modernos é unha das grandes preocupacións actuais dos fabricantes de automóbiles. A seguridade dos sistemas do coche conectado, e non digamos do autónomo, para o seu correcto funcionamento é unha das grandes preocupacións actuais dos fabricantes de automóbiles, e o será en breve de todos nós.

Sistemas de xeolocalización, sondas de presión dos pneumáticos, os sensores de aparcadoiro, iluminación, a información en tempo real da situación do tráfico, etc., ofrecen aos ciberdelincuentes unha ampla información bruta que, ben analizada, pode xerar un patrón, horarios ou localización do condutor. A ameaza é real. Cun sinxelo coñecemento informático e sinxelas ferramentas, o delincuente pode coñecer e manipular a configuración do vehículo e o seu ocupante.

Localizalo para o roubo, manipular os sensores de presión dos pneumáticos e provocar un accidente ou anular o airbag ao seu antollo son accións sinxelas que poden poñernos nun apuro aos condutores. Xa no ano 2015, na conferencia BLACKHAT, Charlie Miller e Chris Valasek, demostraron como hackear un Jeep Cherokee, e en DEFCON o mesmo ano, Marc Rogers e Kevin Mahaffey, ensinaron como facer o propio nun Tesla Model S, o coche conectado por excelencia.

Cos anos, todos desenvolvemos mecanismos para preocupamos pola potencia, o ancho das rodas ou o consumo sexan hábitos innatos, pero somos conscientes da necesidade de ciberseguridade no noso coche? En absoluto. Estamos totalmente desinformados sobre a preparación do coche que imos comprar, descoñecemos o risco que asumimos. Existe algún selo que cualifique a ciberseguridade dos vehículos?

Afortunadamente, aínda non transcendeu que se tomou o control dun vehículo acelerando, freando ou facendo saltar o airbag de forma remota ao antollo do delincuente. Pero todo pode chegar e, co panorama tecnolóxico actual, posible si é posible. A transformación dixital da que goza o sector automobilístico non pode ser allea á ciberseguridade. Para iso buscamos as solucións adecuadas, deseñando un coche ciberseguro e así poder aproveitar as vantaxes que a tecnoloxía nos brinda.

Se algo é real, é que en pouco tempo todas as empresas serán tecnolóxicas, sexa cal for o seu ámbito de actividade. Ter claro o impacto a calquera nivel que supón esta revolución e o efecto habilitador que a seguridade xoga nela, é fundamental á hora de adoptar unha correcta estratexia de dixitalización para o noso negocio.

Desta reflexión nace a actual Emetel, reorganizada en catro áreas ao redor da Dixitalización: Infraestruturas (IoT e conectividade entre outros), Ciberseguridade, Transformación Dixital (smart, big data, analítica) e Servizos (estratexia, xestión do cambio, PMO).

Este escenario, que aparentemente pode resultar difícil ou complexo de abordar, pode converterse nunha oportunidade se se emprende cunha estratexia clara. Minimizar os riscos regulatorios, operacionais e/ou reputacionais, pasan en gran medida por abordar unha estratexia de seguridade aliñada coa estratexia empresarial.

Ante a devandita oportunidade e despois de prepararse longo tempo para facer propios os retos dos clientes, Emetel puxo en marcha unha marca especializada: BE:SEC, que axunta servizos e tecnoloxía, soportada por un centro de operacións de seguridade operativo 24x7 os 365 días do ano, procesos e persoas en constante formación e desenvolvemento, e un conxunto de alianzas que permiten achegar unha visión 360 da seguridade.

Esta nova aposta xa está a dar os seus froitos, como son a Oficina de Seguridade da información da AMTEGA (Xunta de Galicia), os servizos de seguridade do Parlamento de Galicia, ou o aseguramento dos sistemas de Navantia, entre outros. Pero a nosa proposta é realmente diferencial en contornas singulares como os portos intelixentes, o sector industrial e as infraestruturas críticas, onde desenvolvemos solucións para unha dixitalización segura.

***"Minimizar os riscos regulatorios, operacionais e/ou reputacionais, pasan en gran medida por abordar unha estratexia de seguridade aliñada coa estratexia resarial."***

Volver ao sumario

# Seguridade da Internet das cousas (IoT)

Iván Rejón
Head of Strategy Ericsson


A Internet das cousas (IoT) está a emerxer rapidamente como manifestación da visión dunha sociedade en rede onde todo o que se poida beneficiar dunha conexión estará conectado. Con todo, esa gran transformación está apenas comezando, espérase que o número de dispositivos IoT conectados crezan un 21 por cento anual, chegando a 18 mil millóns entre 2016 e 2022.

Internet comezou nun ambiente de confianza mutua, todos podiamos ler, intercambiar ou xerar todo tipo de contidos e información. Pero a IoT está a despegar nun ambiente máis complexo e mesmo ás veces hostil, onde as expectativas do público en xeral, as empresas e os gobernos en materia de seguridade e privacidade son moi altos.

A IoT debe ser seguro desde os seus inicios, protexendo a información persoal, os segredos empresariais, a propiedade intelectual, as infraestruturas críticas, etc. Os reguladores necesitan avanzar garantindo un complexo equilibrio entre a protección da intimidade, salvagarda da seguridade global/rexional e/ou nacional, o estímulo o crecemento económico e ante todo o beneficio á sociedade no seu conxunto.

A IoT xera un novo conxunto de cuestións e retos que todos debemos comprender e afrontar desde os ámbitos tecnolóxico, económico e social

**Ciberseguridade para mil millóns de dispositivos**

A IoT creará a necesidade de xestionar múltiples tipos diferentes de dispositivos, moitos dos cales poden non ser capaces de pedir a un usuario credenciais de inicio de sesión e/ou non poden executar o seu software de seguridade.

Para os hackers, a enorme cantidade e diversidade destes dispositivos aumentará o perímetro de potenciais

*"Internet comezou nun ambiente de confianza mutua, todos podiamos ler, intercambiar ou xerar todo tipo de contidos e información"*

ataques. Gartner estima que para 2020, máis do 25 por cento dos ataques ás empresas farán uso da IoT. O reto de previr os ataques será aínda máis intenso no caso de despregamentos dentro de contornas onde hai unha escasa experiencia técnica, como poidan ser os fogares e as pequenas empresas.

Por outra banda, desde o punto de vista da tecnoloxía operativa, en contornas industriais da IoT o sistemas de control serán máis autónomos e interconectados nalgúns casos a escala global. Por tanto, unha acción de hackeo nestes casos podería ter un impacto real sobre as infraestruturas físicas e o medioambiente aínda superior ao que se produce hoxe en certas catástrofes ambientais.

Por tanto, as infraestruturas, os sistemas físicos con dispositivos sensores non só deben ser capaz de resistir a pirataría directa, senón que tamén debe ser resistente a ataques de todo tipo. A resiliencia cobra unha relevancia esencial nos sistemas en rede.

**Privacidade e seguridade da información na IoT**

A privacidade enténdese e regúlase de diferentes maneiras a través de países e xurisdicións. A atención dos medios de comunicación sobre a privacidade aumentou a conciencia pública, datos aparentemente inofensivos como o consumo de electricidade, por exemplo, pode revelar demasiado sobre os hábitos e/ou a experiencia de consumo. Pero con billóns de sensores por todas partes, a IoT aumentará drasticamente a cantidade de información xerada potencialmente sensible sobre os movementos, actividades, e saúde. As persoas non seremos conscientes dos sensores que nos rodean ou de como os datos combinados de varias fontes poden ser mal utilizados.

Por tanto, mesmo no caso de que as informacións


Volver ao sumario


***"O potencial desencadeado por todo o que está conectado é incrible e supera gradualmente limítelos existentes e imaxinados"***

se encripten, é fundamental protexer os patróns de comportamento de uso e os fluxos de tráfico de datos.

**Seguridade do dispositivo e actualización do software**

Os usuarios actuais esperan seguridade e privacidade mesmo dos dispositivos máis pequenos. Con todo, o deseño dun dispositivo cunha larguísima vida útil, coa alimentación adecuada e un alto nivel de seguridade e resistencia á manipulación pode entrar en conflito co desexo de manter baixos os custos do mesmo.

Por tanto, os dispositivos IoT deben responder á necesidade de asegurar a actualización planificada do firmware e software dos mesmos, superando tanto as limitacións de memoria e capacidade de proceso do deseño inicial como a potencial existencia dalgún virus que infecte o sistema e as aplicacións e tente bloquear estas actualizacións.

**Confianza nos intermediarios – Unha ameaza necesaria?**

Os sistemas IoT baséanse na intermediación e en moitos casos na existencia de redes malladas para reducir o tempo de resposta, o ancho de banda e o consumo de enerxía. Dado que a recepción e a transmisión de radio precisa niveis relativamente altos de potencia, moitos dispositivos IoT están inactivos case todo o tempo e, por tanto, necesitan depender de "proxies" para xestionar peticións e respostas mediante memorias "cache".

Cando son necesarios "proxies" e "gateways", mesmo cando se utilizan protocolos de seguridade como IPsec e TLS, pode haber un incumprimento dos protocolos de intermediación que protexan a integridade da información e o seu fluxo desde o propio dispositivo ao consumidor e/ou o seu centro de control. É dicir, necesítase seguridade na capa de aplicación para facer fronte a estes desafíos.

En conclusión: Imaxine que está a vivir na fascinante sociedade en rede do futuro próximo. O potencial desencadeado por todo o que está conectado é incrible e supera gradualmente limítes existentes e imaxinados.

Neste futuro próximo, o seu espertador fala co seu correo e axenda (pode permanecer na cama un pouco máis se a súa bandexa de entrada permaneceu baleira durante a noite). Ao levantarse, poida que planificase unha saudable sesión de exercicios físicos, pero o ritmo cardíaco rexistrado durante a mesma polo monitor fitness notifica un problema, e comunícase coa oficina do seu médico (envía os datos, e concerta unha cita), a oficina do seu médico comunícase co seu servizo de saúde e/ou provedor de seguro médico, tamén se comunica coa súa oficina, envía unha notificación e facilita o día libre. Ao mesmo tempo, cando sae da casa está dispoñible o seu coche ou o servizo de mobilidade contratado xa que se interactuou coa súa billeteira e cos sistemas de sinalización de xestión de tráfico (O seu coche falaría cos semáforos, pero xa non hai semáforos e posiblemente xa non terá coche en propiedade).

A razón pola que todas estas interaccións flúen e desencadéanse coordinada e intelixentemente é porque que o futuro próximo permitiranos vivir nun mundo con integridade de todos os datos. Non só os datos son sempre tan precisos como poden ser, senón que os sistemas ocuparanse de que todos eles sexan confiables e garantindo que non se modificaron, ben sexa por accidente ou deliberadamente.

Volver ao sumario

# Un enfoque global para a ciberseguridade

Francisco Javier García Lorente
Consultor de Ciberseguridade de everis

an NTT DATA Company

As ciberameazas convertéronse nun impedimento para realizar o noso traballo diario, tanto para as organizacións como para os propios usuarios. Día tras día vemos ataques máis personalizados e específicos, causando unha maior exposición a estes riscos. Por iso temos que ter en conta o importante que é monitorizar estes ataques, saber como actúan a través dun SOC e dar a resposta adecuada e eficiente desde un CSIRT.

## eSOC

Un SOC (Security Operations Center, polas súas siglas en inglés) é un centro de operacións de seguridade especializado no deseño e entrega de servizos administrados que permiten previr e realizar unha monitorización dos incidentes dunha contorna, coa finalidade de reducir riscos e impacto na súa infraestrutura tecnolóxica e no seu negocio. Ademais, conta con información actualizada das vulnerabilidades de seguridade e cos últimos ciberataques rexistrados.

Dentro do uso masivo das novas tecnoloxías e da importancia da información tanto no ámbito público como no privado, as organizacións non poden ser meros espectadores do que ocorre ao redor no que se refire a a protección dos seus sistemas de tecnoloxía da información (TI). Deben ser copartícipes á hora de levar a cabo normas e ferramentas que axuden a que a información permaneza protexida, conseguir a confianza dos cidadáns e minimizar os riscos asociados á súa utilización.

A solución máis habitual para afrontar estes riscos consiste en despregar dispositivos e software de seguridade que nos protexan das ameazas tanto externas como internas.

Con todo, estas medidas, aínda sendo necesarias, non son suficientes para enfocar a solución do problema. Para que os sistemas cumpran a súa función e protexan realmente os activos da organización de posibles ataques é necesario xestionalos, manter as firmas actualizadas, monitorizar alertas e rexistros e realizar as tarefas de operación oportunas para que funcionen correctamente e se adapten á realidade e ao negocio da organización.

***"Un SOC fai posible que as organizacións se poidan centrar no día a día do seu negocio deixando a seguridade lóxica en mans de profesionais cualificados"***

Para iso é imprescindible unha adecuada monitorización, xestión e operación da seguridade que permita responder canto antes e en calquera momento ante un evento de seguridade. Isto pódese conseguir a través dun SOC, que fai posible que as organizacións se poidan centrar no día a día do seu negocio deixando a seguridade lóxica en mans de profesionais cualificados que xestionarán nunha contorna de 24x7 calquera tipo de incidente, alerta ou brecha.

Neste sentido, dentro do catálogo de servizos de ciberseguridade de everis englóbanse os relacionados coa operación e xestión técnica, incluíndo a execución de todas as actuacións preventivas, a operación e configuración da infraestrutura de seguridade, a resposta ante incidentes, a identificación de puntos de mellora e a análise e avaliación de riscos, todo iso para ofrecer a mellor resposta ante posibles ameazas.

A importancia do CSIRT na resposta ás ameazas de seguridade

O Equipo de Resposta a Incidentes de Seguridade Informática (CSIRT, polas súas siglas en inglés) é un centro de seguridade da información, xestión de incidentes e resposta nunha organización. É guiado polo SOC, que actúa como o cerebro dunha organización en temas de ciberseguridade, ademais de supervisar ás persoas, procesos e a tecnoloxía involucrada en todos os aspectos operacionais da ciberseguridade.

Desde agosto o equipo de resposta ante incidentes de everis (everis CSIRT) é oficialmente membro do Foro de Resposta a Incidentes e Equipos de Seguridade (FIRST), principal organización e líder mundial recoñecido en resposta a incidentes. Esta afiliación permítenos responder con maior eficacia a calquera ataque que

Volver ao sumario

comprometa a seguridade ao ter acceso ás mellores prácticas, ferramentas e comunicación co resto de equipos membros tanto de España como doutros países.

## Xestión Integral da ciberseguridade

Actualmente é imprescindible contar cun enfoque integral da ciberseguridade a través de equipos altamente especializados. Por exemplo, en everis contamos con equipos moi cualificados divididos nas áreas de everis CSIRT, o Centro de Operacións de Seguridade (eSOC), o Centro de Hacking Ético e a área de Governance, Risk, Compliance and Business Continuity. Estas áreas intégranse perfectamente para proporcionar unha cobertura eficiente e completa das necesidades de ciberseguridade a nosa propia organización e a todos os nosos clientes en Europa e Latinoamérica.

Ademais, co obxectivo de integrar de forma eficaz os servizos ofrecidos polas distintas áreas, devanditos servizos son agrupados nas seguintes categorías:

- Prevención: auditorías de seguridade, pentesting, análise de vulnerabilidades e outros servizos enfocados á identificación proactiva de vulnerabilidades e debilidades.

- Detección: administrada polo eSOC, proporciona servizos de monitorización interna e externa ademais de threat intelligence.

- Resposta: a área central de everis CSIRT, consolida todas as actividades relacionadas coa xestión de incidentes, a análise e respostas, así como servizos específicos para realizar análises de malware e investigacións forenses.

## Infraestrutura para unha ciberseguridade eficaz

Co fin de poder proporcionar todos estes servizos, everis conta cunha infraestrutura dedicada.

- Laboratorio: área restrinxida e illada, deseñada para prover aos profesionais dunha área onde realizar as investigacións forenses asegurando a confidencialidade dos datos e o cumprimento da cadea de custodia e os requirimentos legais.

- Infraestrutura illada: como parte dos servizos de laboratorio, existe unha infraestrutura totalmente illada deseñada para permitir aos analistas probar con seguridade calquera código sospeitosos e mostras de malware.

- Monitorización 24x7: o equipo de everis é capaz de proporcionar servizos de seguridade xestionados desde o eSOC durante as 24 horas do día, sete días á semana. Ademais conta cunha área restrinxida equipada coa tecnoloxía necesaria para proporcionar estes servizos de forma remota.

- Requisitos especiais de seguridade: neste sector, as certificacións son importantes. everis está certificada polo CNI (Centro Nacional de Intelixencia) para a xestión de información clasificada a nivel nacional, europeo e OTAN, dispondo de toda a infraestrutura, medidas de seguridade e controis necesarios.

***"É imprescindible contar cun enfoque integral da ciberseguridade a través de equipos altamente especializados"***

Volver ao sumario

# A seguridade, cousa de todos

Marcus Fernández
Tesoureiro da Asociación PuntoGal

Nos últimos tempos son moitas as alarmas de seguridade en contornos informáticos que chamaron a atención dos medios de comunicación e alertaron a moitos cidadáns, dándonos a entender a importancia da conservación dos nosos datos persoais con garantías, do mantemento de infraestruturas de telecomunicacións robustas e dunhas políticas de seguridade que minimicen os riscos e faciliten saír do apuro cando todo o demais falle.

Parece que iso do sentidiño é o primeiro que esquecemos no noso día a día, pois tendemos a confiar en sistemas carentes das máis mínimas medidas de seguridade, con software obsoleto, como quedou en evidencia como cando o pasado mes de maio desatouse o ransomware chamado WannaCry, que afectaba principalmente a equipos con Windows XP, e non só iso, senón que a vulnerabilidade principal aproveitanda polo malware correspondía ao protocolo SMBv1, que non só fora corrixida meses atrás, senón que ademais non debería ter afectado a sistemas en produción, xa que tal protocolo só estaba dispoñible a xeito de compatibilidade con vellas redes informáticas, pero non para o seu uso en redes modernas, levando Microsoft advertindo dende hai anos nos seus boletíns de seguridade que non se empregase por motivos de seguridade.

Temos así un caso máis que curioso de seguridade informática na que administradores de sistemas irresponsables, descoidos á hora de configurar redes informáticas e o uso de software obsoleto foi un cóctel perigoso que tivo a moitas empresas en garda durante semanas, expondo a outra grande vulnerabilidade actual: a indefensión ante o ransomware. Resulta evidente que contra un malware que secuestra un equipo informático é moi pouco o que podemos facer despois da infección, e a única solución real é a prevención por dúas canles: mantendo os equipos actualizados e ben configurados; e tendo copias de seguridade dos datos importantes. Este último elemento resultou ser un dos grandes ignorados polas empresas, de aí que estea a proliferar este tipo de ataque informático no que se cifran datos de particulares e empresas para pedir logo un rescate para liberar os contidos. Se temos unha política de copias, estariamos totalmente protexidos tanto ante o ransomware como de posibles fallos que poidamos ter nos sistemas informáticos, como simples avarías até desastres naturais (lume, inundacións...).

En calquera caso, manter a seguridade dos datos que teñamos na empresa ou no fogar, e ter os nosos sistemas protexidos, só é unha parte da ecuación, xa que tamén é preciso que nas estradas polas que se move a información vaia todo ben, algo que non sempre é valorado polo usuario até que algo sae mal. Precisamente do último tivemos varios exemplos na nosa comunidade, como foron os ataques informáticos padecidos polas compañías de telecomunicacións R e Ocean's, que deixaron aos seus clientes durante horas sen servizo, o

***"As actuacións malintencionadas contra elementos críticos son algo a ter moi en conta, e debería chamar á reflexión sobre a necesidade de contar cada vez con infraestruturas máis sólidas."***

Volver ao sumario

***"A diversidade da Internet é tal que a súa principal bondade tamén é un punto feble"***

que é un problema extraordinariamente grave, xa que a incomunicación pode ter repercusións moi serias; e tamén foi moi sonado un ataque de denegación de servizo a Dinahosting, empresa de hospedaxe de páxinas web moi popular na nosa terra, que como consecuencia tivo que numerosas páxinas web galegas non estaban accesibles (entre as que había algún medio de comunicación). Vemos nestes casos que as actuacións malintencionadas contra elementos críticos son algo a ter moi en conta, e debería chamar á reflexión sobre a necesidade de contar cada vez con infraestruturas máis sólidas, xa que a nosa dependencia das telecomunicacións é cada día maior, e en moitas ocasións traballamos contra sistemas remotos, de xeito que se as conexións fallan non é posible operar de ningún xeito.

A preocupación polas infraestruturas de comunicacións é algo moi serio, tanto a nivel físico (hai anos o norte de España quedou sen servizo de telefonía por mor dunha avaría provocada nun punto crítico da rede dun operador, demostrándose que a súa arquitectura era claramente deficiente) como a nivel lóxico, e dende relaxadas políticas de actualizacións até pequenos fallos de seguridade permiten que un ataque de denegación de servizo a un dos grandes sistemas de servidores de nomes da Internet (DNS) afecten a boa parte dos EE.UU. e outras partes do mundo facendo que dende Twitter até Paypal, pasando pola PlayStation Network, tivesen problemas de funcionamento, ou sexa, que a historia de que a Internet está creada para soportar ataques nucleares demostra día a día ser un conto, e na práctica continuamos a ter moitos puntos vulnerables, xa que a Rede en si mesma deseñouse partindo dun nivel de confianza propio dos contornos educativos e de investigación, e non pensando nunha xungla na que conviven entidades bancarias, usuarios particulares, ordenadores persoais, establecementos comerciais, servizos de pagamento, dispositivos móbiles e toda unha infinidade de obxectos conectados. A diversidade da Internet é tal que a súa principal bondade tamén é un punto feble. A Rede non podería chegar a desenvolverse en tan poucas décadas se non fose así, pero agora temos que coidar cada vez máis tal infraestrutura, facerlle o mantemento oportuno e actualizala paulatinamente como tamén facemos coas vías de comunicación convencionais.

Non só temos que construír autoestradas para facilitar unha circulación fluída, senón que tamén é preciso deseñar as vías para emerxencias, e entre os responsables das infraestruturas é imprescindible a cautela, para que non se repitan casos como o de Google o pasado verán, que deixou a máis de 8 millóns de xaponeses sen acceso á Internet por ocupar accidentalmente un rango de enderezos IP correspondente a un dos principais provedores de acceso do país asiático, algo que non é a primeira vez que acontece a nivel mundial, de xeito que xa temos visto países enteiros desaparecer da Internet durante horas por mor de erros humanos, algo que non debería acontecer baixo ningún concepto.

Redeseñar a Internet dende cero, poñendo a seguridade nos alicerces non é unha opción, pero si fomentar unha cultura da ciberseguridade, para que cada vez os particulares coidemos mellor dos nosos datos, os usuarios da Rede empreguemos equipos actualizados e sigamos pautas de uso seguras, os fabricantes manteñan actualizados ao máximo posible os seus produtos para que non espallen vulnerabilidades que poidan ser aproveitadas na nosa contra e incluso que se establezan mellores protocolos que nos vaian guiando na dirección correcta, para que a seguridade no mundo dixital non sexa máis preocupante que a do mundo que nos rodea.

Volver ao sumario

# O futuro da ciberseguridade: Intelixencia Artificial?

Luis Pérez Freire, Director General
Juan González Martínez, Responsable de Seguridade e Privacidade
Carlos Giraldo Rodríguez, Investigador

Cando William Gibson escribiu *Neuromante* no ano 1984, anos antes do nacemento da *World Wide Web*, non foi soamente quen de anticiparse a un mundo hiperconectado, empregando o termo ciberespazo, senón que predixo tamén os problemas de ciberseguridade asociados. Na novela, Case, o antiheroe e *hacker* (*cybercowboy* no texto de Gibson) é contratado para vulnerar a seguridade dun sistema crítico dunha gran corporación. Este tipo de ataques tecnicamente avanzados, empregando o ciberespazo, ben financiados e auspiciados por gobernos ou grandes corporacións non nos é descoñecido hoxe en día, de feito referímonos a eles como Ameazas Avanzadas Persistentes (*APT, Advanced Persistent Threats*).

Na novela de Gibson, as corporacións protexen os seus sistemas máis críticos empregando ferramentas de detección e neutralización de ataques, coñecidas polo acrónimo ICE (*Intrusion Countermeasures Electronics*). O equivalente na nosa realidade serían os sistemas de detección ou prevención de intrusión (*IDS, Intrusion Detection System – IPS, Intrusion Protection System*). En Neuromante, as versións máis avanzadas de ICE, denominadas Black ICE, capaces non soamente de evitar o ataque, senón de chegar a matar a persoa que o realiza, son controladas mediante Intelixencia Artificial. Aínda que dende o punto de vista da ciberseguridade o obxectivo non é matar o atacante senón identificar, deter e extraer intelixencia do ataque, estaba Gibson no certo? Que papel xoga ou podería xogar a Intelixencia Artificial no campo da ciberseguridade e en particular nos sistemas de detección de intrusión?

**Aplicación da Intelixencia Artificial á Ciberseguridade**

Por ciberseguridade entendemos o conxunto de tecnoloxías empregadas para protexer ás redes e os seus nodos de ataques, danos e accesos ou modificacións non autorizados. Entre estas tecnoloxías destacan os sistemas de detección de intrusións (IDS) tanto en redes como en nodos da rede. Actualmente existen tres tipos de IDS en función das tecnoloxías subxacentes na detección: baseados en sinaturas, baseados en detección de anomalías, e sistemas híbridos.

***"A investigación está a avanzar con rapidez na dirección de acadar cada vez mellores niveis de sensibilidade, proporcionando un alto grao de anomalías detectadas e unha baixa taxa de falsas alarmas"***

Os sistemas baseados en sinaturas empréganse especialmente para detectar ataques coñecidos. Por exemplo: un virus que contén un determinado ficheiro ou un ataque de SQL Injection que contén unha determinada cadea de texto coñecida. Estes sistemas requiren que as sinaturas sexan actualizadas constantemente, e por suposto non poden detectar ataques non coñecidos (*zeroday attacks*). Os sistemas baseados en detección de anomalías identifican patróns de comportamento que representen unha desviación da "normalidade". Estes sistemas son máis potentes que baseados en sinaturas xa que permiten detectar ataques descoñecidos a priori polo sistema. Outra importante vantaxe é que a "normalidade" defínese para cada sistema, dificultando aos atacantes a preparación de ferramentas que pasen desapercibidas polo IDS. Os sistemas híbridos combinan a detección baseada en sinaturas coa detección baseada en anomalías. Na práctica apenas existen sistemas baseados en detección de anomalías puros.

A detección de anomalías pódese realizar empregando distintas técnicas, como cálculos puramente estatísticos e minería de datos (*data mining*), pero as técnicas baseadas en Intelixencia Artificial, como *Machine Learning* (ML), estanse a amosar especialmente prometedoras. Actualmente atopámonos nun momento de maduración da tecnoloxía, polo que as técnicas ML aínda poden presentar unha taxa alta de falsas alarmas, dificultando deste xeito o traballo dos analistas de seguridade, pero a investigación está a avanzar con rapidez na dirección de acadar cada vez mellores niveis de sensibilidade, proporcionando un alto grao de anomalías detectadas e unha baixa taxa de falsas alarmas.

Volver ao sumario

**A investigación en Gradiant, Red ICE**

Aproveitando a experiencia de Gradiant no deseño de sistemas de *Machine Learning* e outras solucións de Intelixencia Artificial, e no desenvolvemento de tecnoloxías que melloren a ciberseguridade, recentemente vimos de completar unha proba de concepto dun motor de Machine Learning para validar a aplicación de técnicas de ML á detección de intrusións.

O primeiro paso foi decidir que fontes de datos se usarían como entrada para o sistema. Antivirus, devasas, sistemas de detección de intrusións, proxies, xestión de eventos e información de seguridade (*SIEM, Security Information Event Management*)... Hai moitos tipos de fontes de datos no eido da ciberseguridade. Para dotar á nosa plataforma de información válida e confiable, seleccionamos software de referencia de código aberto que cobre diferentes obxectivos: IDS de rede (Suricata e BRO), IDS de host (OSSIM) e os logs do proxy de rede (Squid).

O segundo paso foi definir unha linguaxe común normalizada á que transformar as distintas fontes de datos. A linguaxe elixida está inspirada en Apache Spot Open Data Model, unha iniciativa que está a dar os primeiros pasos cara a unha taxonomía común para describir os datos de telemetría de seguridade utilizados para detectar ameazas.

Unha vez normalizados os datos pódense introducir no motor de Machine Learning deseñado por Gradiant, Red ICE. Ese motor incorpora distintos algoritmos de aprendizaxe automático desenvolvidos por Gradiant, orientados á detección de intrusións. A modo de exemplo, mencionar un algoritmo que modela o rol de cada host na rede, é dicir, se o host é principalmente un produtor de datos ou un consumidor de datos. A continuación, o algoritmo busca cambios de rol para detectar posibles intrusións.

Outra funcionalidade soportada polo motor de Gradiant é o resumo dos rexistros de eventos. Os sistemas de detección de intrusos adoitan activar miles de alertas cada día. Debido a esa cantidade de información, as alertas importantes poden pasar desapercibidas para o administrador da rede. A configuración personalizada do IDS ou o post-procesamento de saída son tarefas custosas que requiren coñecementos expertos. Por iso, aplicáronse técnicas de minería de patróns e de clusterización de textos para resumir as alertas e resaltar os valores atípicos das mesmas.

As alertas tamén foron analizadas con técnicas de minería de procesos. O algoritmo xera modelos de procesos que representan estratexias de ataque. A continuación, o fluxo

***"Coa aplicación da Intelixencia Artificial espérase unha nova xeración de produtos que melloren a seguridade ao mesmo tempo que diminúan os custes"***

de datos pódese analizar en tempo real para detectar un proceso de ataque e reaccionar ao mesmo antes de que o ataque se complete.

Os seguintes pasos para ampliar a capacidade do sistema pasan principalmente por ampliar as fontes de información, incluíndo fluxos de datos de rede, capturas de paquetes de rede e información de antivirus e rexistros de actividade de sistema. Os bos resultados obtidos na proba de concepto serven como indicador da conveniencia de empregar técnicas de Intelixencia Artificial á ciberseguridade. Para continuar con esta liña de investigación, Gradiant, dentro dun potente consorcio europeo, ven de solicitar recentemente financiamento á Unión Europea a través do programa de apoio a investigación H2020.

**O futuro**

Paseando por calquera das feiras de seguridade informática é doado ver que os principais fabricantes, principalmente os emerxentes, están a apostar pola Intelixencia Artificial para mellorar as capacidades dos seus produtos, xa sexan antivirus, sistemas de detección de intrusións, sistemas de xestión de eventos de seguridades, devasas, detectores de spam, etc., pero polo de agora son fundamentalmente pequenas funcionalidades construídas sobre o núcleo dos seus produtos. Os algoritmos de Intelixencia Artificial, pola súa capacidade de aprendizaxe, preséntanse como unha tecnoloxía axeitada para un problema, os ciberataques, que evolucionan constantemente para evadir as ferramentas de detección. Buscamos, por tanto, invertir o paradigma clásico da ciberseguridade segundo o cal as medidas defensivas sempre van por detrás dos atacantes. A aplicación da IA á ciberseguridade é un campo emerxente, aderezado tamén, por suposto, polo efecto no marketing do Machine Learning, Deep Learning, etc. Así e todo, coa aplicación da IA espérase unha nova xeración de produtos que melloren a seguridade ao mesmo tempo que diminúan os custes necesarios para a súa xestión.

Volver ao sumario

# Retos da ciberseguridade

Jorge García Carnicero, Xefe de desenvolvemento empresarial ciberseguridade de Minsait

O volume e sofisticación das ameazas veu incrementándose de forma exponencial durante os últimos anos, convertendo a misión de protexer o footprint dixital dos clientes nunha tarefa realmente complexa. Este feito, xunto coa revolución que está a sufrir o modelo TI das compañías empuxado polos procesos de Transformación Dixital dos negocios (canles, novos negocios e relación con clientes, principalmente), fai que a aproximación tradicional das organizacións á ciberseguridade non cubra as necesidades reais de protección dos negocios.

Na primeira metade do 2017, as empresas foron máis propensas aos ciberataques, xa que un de cada tres equipos foi obxectivo, segundo sinala Kaspersky Lab no seu informe "Threat landscape for industrial automation system in H1". O punto álxido de actividade cibercriminal tivo lugar no mes de marzo, momento a partir do cal a proporción de equipos atacados foi reducíndose progresivamente ata o final do período.

Segundo o informe "Threat landscape report Q2" de Fortinet:

- 62 millóns de detección de malware
- 677,000 volume diario promedio
- 16.582 variantes de malware total
- 2.534 familias diferentes de malware
- 18% de las empresas viron malware móbil

Na primeira metade do ano, o mundo enfrontouse a unha epidemia de ransomware que tamén afectou as empresas industriais. Segundo o estudo de Kaspersky Lab ICS CERT, o número de equipos ICS (industrial control systems) únicos atacados por troyanos cifradores incrementouse e triplicou ata o mes de xuño.

As principais estatísticas de ransomware durante a primeira metade do 2017 incluídas no informe son as seguintes:

Os equipos ICS en 63 países de todo o mundo foron obxectivo de numerosos ataques de ransomware de cifrado, entre eles os máis coñecidos foron as campañas de WannaCry e ExPetr.

Entre o top 10 das familias de troianos de cifrado inclúense tamén Locky e Cerber, en activo desde 2016 e situándose entre as máis rendibles para os cibercriminais.

A seguinte figura amosa a relación impacto/probabilidade dos ciberataques, dentro dos riscos globais considerados polo World Economic Forum. Como pode observarse, o WEF sitúa a este risco entre os máis significativos.

Desde esta óptica, faise necesario explorar novas aproximacións e modelos de ciberseguridade que dean resposta ás necesidades reais.

## Non existe Transformación Dixital sen ciberseguridade

Os principais retos que afrontan as compañías á hora de protexerse teñen que ver tamén coa evolución e as tendencias do negocio, a denominada Transformación Dixital. Actualmente identifícanse 4 correntes:

• Cloud Computing, e filosofía DevOps: Caracterízase principalmente polo crecente uso de servizos cloud, polo uso que fan deles os seus empregados e colaboradores, así como pola axilidade que estes demandan á hora de que as TI satisfagan os requisitos de ciberseguridade (resiliencia e redución do risco) sen que iso supoña un freo ao estafe to market do negocio. Moi relacionado co cloud, o modelo as a service tamén expón un gran reto despois de que o impacto que pode ter un incumprimento dos ANS de seguridade por parte do provedor de servizos, en moitos casos non pode ser compensado por penalizacións económicas, como é o caso das fugas de información (Sony, Target, Panama Papers, Cablegate/ wikileaks, etc.)

• Internet das Cousas e ciberseguridade industrial (OT). Os dispositivos conectados son un dos alicerces da transformación dixital dos procesos de negocio das compañías e dos produtos que estas comercializan xa que permiten obter información de valor sobre a cal tomar decisións de optimización, oportunidade, etc. Esta novo paradigma expón novos vectores de ataque que se deben protexer, os cales, dependendo da criticidad dos elementos, poden resultar de extrema importancia. A problemática destas contornas non está ao alcance das empresas de ciberseguridade ?tradicionais? (pure players) xa que non basta coñecer as medidas de ciberseguridade, senón tamén entender a funcionalidade industrial do dispositivo e o seu funcionamento técnico. As empresas do sector en xeral non están preparadas para afrontar este enorme reto.

• Omnicanalidade e adopción do móbil como canle principal. Os retos neste aspecto teñen que ver con garantir e, sobre todo, facilitar unha identidade dixital que contribúa á mellor experiencia do cliente, que sexa sinxela (por exemplo, biometría) e válida para todas as canles e servizos. Ao mesmo tempo, tamén é necesario garantir a seguridade dos dispositivos en si mesmos, neste caso os dispositivos móbiles cuxo boom en materia de vulnerabilidades e incidentes estamos a comezar a experimentar.

• Big Data. Hoxe todos os datos do negocio camiñan cara ao data lake, abandonando as contornas de base de datos tradicionalmente protexidos aínda que sexa con medidas básicas de ciberseguridade. A paradigma do Big Data expón grandes oportunidades en materia de ciberseguridade posto que a explotación de enormes series históricas de datos capturados permite inferir e

Volver ao sumario

anticipar incidentes con cada vez maior precisión. Pero tamén expón grandes retos relacionados coa protección dos datos almacenados e a limitación do acceso de usuarios e administradores así como a tokenización (anonimización) dos mesmos para evitar un tratamento inadecuado desde o punto de vista da privacidade, mantendo a utilidade estatística para o negocio.

### Que obxectivos se perseguen? Prevención e, agora sobre todo, resiliencia

Tradicionalmente traballouse a seguridade preventiva tratando de minimizar o risco de materialización das ameazas. Con todo, a experiencia destes últimos anos demostra que cada vez son menos efectivas estas medidas e que é necesario "convivir co inimigo" (as ameazas vanse a materializar) e por tanto é necesario despregar medidas que aseguren: primeiro, que as organizacións serán conscientes do incidente canto antes e segundo, que o negocio está preparado para resistir e manter a actividade coa máxima normalidade a pesar do ataque.

### A que nos enfrontamos

O mesmo CNN-CERT prognostica, unha vez máis, un incremento na capacidade dos atacantes para sortear os sistemas de seguridade e evitar ser detectados. Os ataques están a volverse cada vez máis dirixidos, utilizando técnicas de enxeñaría social, afectando os sistemas de copia de seguridade, que fai imposible en moitos casos a recuperación da información. Tanto o perfil dos ciberdelincuentes como a natureza dos ataques supuxeron unha sofisticación exponencial dos desafíos, sumando enormes capacidades tecnolóxicas cun uso cada vez máis eficaz da enxeñaría social. Todo iso tradúcese nun crecemento constante do nivel de risco que supoñen ditas actividades fraudulentas.

As ameazas de seguridade que máis relevancia están a ter desde o punto de vista da dificultade de detección e da gravidade dos incidentes provocados son:

• Ameazas Persistentes Avanzadas (APT): Ataques a longo prazo baseados en software malicioso e intervención humana continuada que, de forma sigilosa, van penetrando progresivamente nos sistemas de información das compañías sorteando os perímetros de seguridade sen ser detectados e accedendo á información máis confidencial das organizacións. Cando son detectadas adoita ser tarde.

• Ramsomware. Táctica empregada por bandas criminais que mediante a infección con código malicioso (e enxeñaría social como método de infección), secuestran dispositivos e información e piden rescates pola súa liberación.

• Phishing avanzado, mediante técnicas de enxeñaría social créanse ataques personalizados normalmente dirixidos cara a C levels das compañías

### A interconexión de Sistemas de Control Industrial

A inseguridade do software vólvese especialmente delicada cando se trata de software para Sistemas de Control Industrial, moi especialmente cando tales sistemas se atopan interconectados a través de internet. Un software inseguro, instalado nun sistema determinado, xera inseguridade en todos aqueles a os que se conecta.

### Os custos dos ciberincidentes e da súa xestión

É indubidable que as brechas de seguridade teñen un custo global, derivado de varios custos parciais: económicos directos, de servizo, de reputación e imaxe, por sancións, etc.

España recibiu ataques especialmente dirixidos ás industrias da Defensa, compañías Tecnolóxicas e entidades significadas do Sector Público.

### Acompañan adecuadamente normativa e lexislación?

Un último punto a ter en conta en canto ás tendencias de ciberseguridade son os cambios na lexislación, principalmente as novas directivas e regulamentos no ámbito europeo. Por unha banda, o novo regulamento de protección de datos pretende devolver aos cidadáns o control dos seus datos persoais e garantir en toda a UE uns estándares de protección elevados e adaptados á contorna dixital. Tamén inclúe novas normas mínimas sobre o uso de datos para fins xudiciais e policiais.

Doutra banda, a Directiva NIS (Directiva sobre seguridade das redes e os sistemas de información) establece obrigacións de seguridade para os operadores de servizos esenciais (en sectores críticos como a enerxía, o transporte, a saúde e as finanzas) e os provedores de servizos dixitais (mercados en liña, motores de procura e servizos en nube).

Dado que o panorama das ameazas de seguridade cibernética evoluciona rapidamente, é necesario implementar rapidamente a Directiva. En vista dos prazos inminentes para a súa transposición á lexislación nacional (ata o 9 de maio de 2018) e para a identificación de operadores de servizos esenciais (ata o 9 de novembro de 2018).

### Acompañan adecuadamente normativa e lexislación?

Un último punto a ter en conta en canto ás tendencias de ciberseguridade son os cambios na lexislación, principalmente as novas directivas e regulamentos no ámbito europeo. Por unha banda, o novo regulamento de protección de datos pretende devolver aos cidadáns o control dos seus datos persoais e garantir en toda a UE uns estándares de protección elevados e adaptados á contorna dixital. Tamén inclúe novas normas mínimas sobre o uso de datos para fins xudiciais e policiais.

Doutra banda, a Directiva NIS (Directiva sobre seguridade das redes e os sistemas da proposta de valor de Minsait.

Minsait desenvolveu unha proposta de valor para facer fronte a estes retos mediante un conxunto de solucións orientadas a cubrir as necesidades dos clientes.

FEE(P) aglutina o conxunto de servizos SOC e infraestruturas de protección que os departamentos de IT das compañías necesitan para cubrir estas ameazas. Coas solucións (F)EEP Dixital Identity Minsait cobre as necesidades de identidade dixital da industria 4.0, combinando tecnoloxía biométrica, de verificación de documentos e infraestrutura de clave pública.

Volver ao sumario

# Camiñando cara o novo Regulamento Europeo de Protección de Datos en prol da ciberseguridade

Giovanni Giardina
Presidente de INEO, Asociación de Empresas de Tecnoloxía de Galicia

Conta atrás para a aplicación do Regulamento Xeral de Protección de Datos, tamén coñecido coas siglas en inglés "GDPR". Con esta normativa europea, chegan novos dereitos, obrigacións e responsabilidades para os que debemos estar preparados. Tamén chegan novas garantías en materia de ciberseguridade para as empresas e os cidadáns.

Como sabedes, a nova regulación europea de protección de datos entrou en vigor no noso país o pasado 25 de maio de 2016, aínda que non será ata o vindeiro 25 de maio de 2018 cando será de obrigado cumprimento para todas as empresas que traballan con datos persoais de cidadáns da Unión Europea. Estamos pois, nun período de adestramento no que debemos analizar e avaliar os compromisos que traerá esta normativa, que tamén virá acompañada de novas oportunidades para as empresas tecnolóxicas galegas.

INEO, a asociación que represento, naceu para axudar ás empresas TIC a consolidarse como un sector de importancia vital para a economía da rexión, a través da creación de riqueza, a innovación e o aumento da competitivade e productividade dos demais sectores empresariais. O novo Regulamento Europeo será de gran importancia para cumprir con estes obxectivos, xa que abrirá un novo escenario para desenvolver solucións e servizos aliñados coa nova normativa que axuden ao tecido empresarial e ao conxunto da sociedade a estar máis protexidos e seguros.

Non procede enumerar todos os cambios aos que nos enfrontaremos nas nosas empresas, pero si que creo necesario facer fincapé nalgunhas das novidades que marcarán a estratexia que teremos que implementar dende o noso sector.

## Máis transparencia e un maior compromiso pola privacidade

Na nova normativa se reforzan os principios de "*responsabilidade proactiva*" e o de "transparencia", que esixirán un maior compromiso de cara a privacidade e a protección de datos dos cidadáns e das empresas. Estes traerán consigo a obrigatoriedade na aplicación de medidas técnicas e organizativas que garantan que

o tratamento dos datos estase a levar a cabo conforme ao Regulamento. Ademais, haberá cambios na forma de obter o consentimento, de forma que este será inequívoco e nalgúns casos explícito, o que dará lugar a unha revisión no xeito no que este se obtén actualmente e tamén na forma de documentalo adecuadamente. Tamén haberá modificacións na información que proporcionamos sobre como se tratan os datos dos interesados e os avisos de privacidade.

***"O Regulamento Europeo abrirá un novo escenario para desenvolver solucións e servizos aliñados coa nova normativa"***

## "Dereito ao esquecemento" e "dereito á portabilidade", novas ferramentas de protección para os cidadáns

O Regulamento blinda aínda máis a protección dos datos persoais dos cidadáns e por iso introduce novas ferramentas que melloran o control dos mesmos. Un deles é o "*dereito ao esquecemento*" polo que os interesados poderán solicitar o borrado definitivo dos seus datos,

Volver ao sumario

tanto por parte de procuradores de internet como de calquera provedor de servizos online.

Por outra banda, poderase reclamar o dereito á portabilidade dos datos, unha forma avanzada do dereito de acceso, que permitirá aos cidadáns que proporcionasen os seus datos a un responsable, recuperar eses datos nun formato que lle permita o seu traslado a outro responsable. Isto facilitará a transmisión de datos a outras empresas.

### O "Delegado de Protección de Datos" e outras medidas de responsabilidade activa

As empresas tecnolóxicas teremos unha responsabilidade activa co "GDPR" baseada na prevención. Non só debemos implementar medidas que aseguren o cumprimento dos principios, dereitos e garantías que establece a nova normativa, senón que debemos anticiparnos ás infraccións e traballar nas tarefas de prevención. Por este motivo, o Regulamento fixa un catálogo de medidas entre as que se atopan: análise de riscos, rexistro de actividades de tratamento, protección de datos dende o deseño e por defecto, medidas de seguridade, notificación de "violacións de seguridade dos datos", avaliación de impacto sobre a protección de datos e tamén unha novidosa figura denominada "delegado de protección de datos". Este último, coñecido coas siglas "DPO" (*Data Protection Officer*), poderá ser persoal interno da empresa ou un asesor externo, e será o encargado de informar, asesorar e supervisar o cumprimento do Regulamento.

### Unha única autoridade de protección de datos

Outra das novidades é o sistema de portelo único. Grazas a este, todos aqueles que traten datos de cidadáns de calquera Estado membro da Unión Europea, terán de interlocutora a unha única autoridade de protección de datos.

Así mesmo, a autoridade de protección de datos non só tratará os asuntos de índole nacional, senón que tamén poderá valorar se o caso que se expón transcende as fronteiras do Estado. Neste suposto, poñerán en contacto ás autoridades de cada un dos países afectados para coordinar a resolución do caso.

### Responsabilidades e sancións severas

Que ocorre no caso de que se incumpran as normas? Pois as empresas enfrontaríanse a multas de ata 20.000.000 euros ou ao 4% da súa facturación e, por suposto, o descoñecemento non exime do seu cumprimento.

### Oportunidades do noso marco normativo

Agora temos unha oportunidade perfecta para anticiparnos á entrada en vigor deste Regulamento. A tal efecto, debemos facer unha preparación interna e asesorarnos, establecer medidas e protocolos de actuación, analizar os posibles riscos, capacitar e formar ao noso persoal… pero, por outra banda, debemos facer tamén unha labor divulgativa informando aos nosos clientes e ao tecido empresarial en xeral das obrigas, posibles sancións e tamén das garantías e proteccións que este novo marco normativo supón para a súa seguridade e privacidade. Dende INEO, xa o estamos a facer.

***"As empresas tecnolóxicas temos una responsabilidade activa baseada na prevención. Preparémonos xa para cumprir coas nosas obrigas"***

Volver ao sumario

# Anatomía dun ciberataque

Alexandre Tovar López-Amo
Product Manager IPM

O 1 de outubro do 2003, Gabe Newell, presidente de Valve Corporation, seguía tendo o problema de enfrontarse á decisión de comunicar ou non o atraso na publicación da secuela do exitoso videoxogo Half-Life. Nun momento delicado, como compañía de videoxogos que aínda non se convertera no xigante valorado en 4 billóns de dólares que é hoxe en día, o seu fundador era consciente de que o xogo necesitaría outro ano para estar terminado. Transmitir ese atraso podía significar un dano á reputación da empresa e afectar negativamente as vendas. Durante os últimos meses, Newell negouse a informar á prensa, mesmo cando a data oficial do lanzamento do xogo xa fora excedida. Aquela mañá, a decisión continuaba planeando sobre a súa cabeza e era o principal motivo de preocupación dentro das oficinas. Ao día seguinte, a empresa tiña un problema moito maior. Un co potencial de provocar o seu peche para sempre. Ás 11 da noite, o presidente de Valve Corporation enviaba un comunicado pedindo axuda á comunidade: Half-Life 2, o xogo que marcaría o seu futuro como compañía, fora filtrado a Internet. O código fonte do xogo, os niveis xogables, os personaxes, as armas, as localizacións? Todo fora roubado e publicado. A noticia expandiuse a gran velocidade. Miles de persoas descargáronse os arquivos. A medida que se pechaban páxinas web e

***"Este ataque aínda se encadraba dentro da visión romántica da intrusión informática simbolizada na figura do adolescente solitario, superdotado e autodidacta."***

ligazóns cos devanditos contidos, xurdían dez máis no seu lugar.

Tres semanas antes, un mozo alemán empezara a descarga dos arquivos do xogo. Previamente, só por curiosidade, logrou atopar a maneira de acceder á rede interna de Valve Corporation e navegar por ela buscando información sobre o longamente esperado xogo. Ninguén se deu conta da intrusión. Ninguén se deu conta do visitante, que estivo días esculcando pola rede da empresa. Ninguén detectou o envío ao exterior de ficheiros relacionados co código do xogo e ninguén puido trazar, a posteriori, a ruta do mozo polas entrañas informáticas da compañía. Tampouco se atoparon evidencias nin probas inculpatorias. Só despois de varios meses, foi o mesmo mozo o que contactou co presidente de Valve Corporation para desculparse pola súa acción.

Volver ao sumario

***"A expectativa dos usuarios respecto da tecnoloxía cambiou enormemente. Queren acceso sen límites aos recursos e á información"***

El mesmo confesou o seu acceso e como o fixo. O xogo, por certo, foi un éxito de vendas cando saíu ao mercado a finais do 2004.

Este ataque aínda se encadraba dentro da visión romántica da intrusión informática simbolizada na figura do adolescente solitario, superdotado e autodidacta. O patrón do ataque era similar ao doutros: investigación, detección do punto débil, contacto, intrusión, exploración e extracción. As compañías empezaron a blindarse e a protexer o seu perímetro para evitar os dous primeiros pasos dos ataques. E tiveron razón, polo menos durante un tempo. En catorce anos as cousas cambiaron moito. Hoxe, os ataques son máis sofisticados. Están dirixidos, a súa motivación principal é monetaria e atacan desde o interior das organizacións. A seguridade perimetral nun mundo Cloud non ten sentido xa que as fronteiras da empresa expandíronse máis aló dos límites que somos capaces de administrar. E é aquí onde a velocidade de detección e a analítica pode axudarnos.

Para cada un dos pasos que segue un ataque, existe unha forma de defenderse. Con todo, non debemos esquecer que non hai unha única ferramenta máxica que nos ofreza todas as solucións que necesitamos.

Un ataque vai tentar establecer un punto de apoio para poder desenvolverse e a forma máis fácil de acceder a unha organización é enviando un correo electrónico a un empregado. Continuamos sendo, como individuos, o elo máis débil con relación á seguridade. O labor das empresas vén centrando en desenvolver procesos e adquirir tecnoloxía para o despregamento automático de actualizacións que impidan aos atacantes aproveitar fallos de seguridade no software. No entanto, o mellor investimento e tamén a máis barata segue sendo a educación dos empregados para que saiban detectar e evitar os intentos de intrusión, apropiación de identidade e roubo de contrasinais que recibirán nas súas caixas de correos de correo. Preto do 70% dos intentos de acceder a información comezan cun e-mail e bastan 60 segundos desde que se executa un arquivo adxunto ou se accede a un URL infectada para que un ransomware como Wannacry encripte a máquina afectada.

Se o ataque logrou entrar na organización, agora necesita afianzarse e estenderse. Ningunha das solucións de seguridade perimetral pode impedilo. Podemos usar métodos de autenticación e establecer ferramentas de seguridade para reducir accesos non autorizados e para controlar movementos sospeitosos dentro da nosa rede que poidan indicar que se está propagando unha intrusión. Dado que moitos dos ataques necesitan conectarse ao exterior para descargar parte do código que necesitan para cumprir o seu obxectivo, debemos ser capaces de detectar este tipo de comunicación.

Chegado o caso de que a ofensiva conseguise evitar ser detectado é o momento para o intruso de exfiltrar a información e manterse dentro do sistema para futuros ataques. Monitorando a nosa rede temos a posibilidade de detectar patróns e comportamentos anómalos dentro das comunicacións normais da empresa. Coñecendo como funciona a nosa rede é cando detectaremos usos non habituais de protocolos de comunicación e investigando devanditos usos é cando poderemos descubrir ataques en curso.

A expectativa dos usuarios respecto da tecnoloxía cambiou enormemente. Queren acceso sen límites aos recursos e á información. Non importa onde estean ou con que dispositivo executen os servizos que necesitan para facer o seu traballo. Isto eliminou o concepto de seguridade perimetral e está a mover o foco cara a sistemas de análises interconectadas e potenciadas por IA e Big Data. As organizacións deben ser capaces de previr a maior cantidade posible de ameazas para que non accedan ao interior da súa rede, sen esquecer que é moi posible que xa estea a suceder algo dentro da súa organización. E por organización habemos de entender que estamos a falar de que calquera dato ou servizo, non importa o lonxe que estea fisicamente das nosas oficinas.í onde se atopen, continúan sendo nosa empresa. Por iso debemos protexelos da mesma forma que protexemos os nosos servizos on-premise.


Volver ao sumario

# GDPR, unha regulación europea para o mundo dixital

Mauricio Gumiel
Director de Ciberseguridade, Oracle

Son moitas as regulacións e decretos que estableceron criterios para tratar a confidencialidade da información, a protección dos datos, a vixilancia e control do acceso aos mesmos. Con todo, non é ata agora que se pon de manifesto a necesidade de implementar medidas que, con carácter obrigatorio, forcen ás organizacións a redeseñar os seus sistemas de información.

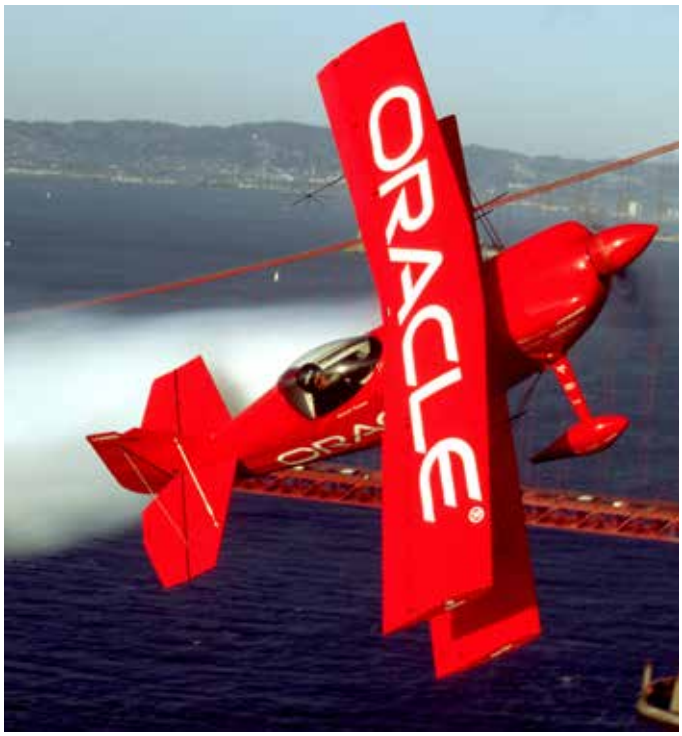
Co propósito de garantir que o dereito fundamental á protección de datos se aplique de modo coherente en todos os países que conforman a UE, as autoridades europeas viñeron traballando no desenvolvemento dunha normativa que, coñecida como Regulamento Xeral de Protección de Datos europeo ou GDPR -polas súas siglas en inglés-, entrará en vigor o próximo 25 de maio de 2018, nos 28 países da UE.

En España, a nova regulación sobre privacidade e impacto nos negocios e procesos dixitais derrogará a actual LOPD -Lei Orgánica de Protección de Datos- e sentará as bases da harmonización das regras de uso dos datos persoais e a privacidade dos cidadáns no conxunto do territorio europeo.

Como novidade, a futura normativa prevé a designación en todas as organizacións dun Data Protection Officer -DPO-, encargado de implantar medidas eficaces, de realizar verificacións periódicas e de avaliar os impactos das mesmas. Ademais deberá establecer as vías necesarias para avalar a privacidade por deseño e por defecto, ademais do control e rexistro de tratamento.

Igualmente, os CSO, CISO, CIO de compañías privadas e administracións públicas deberán estar moi atentos para cumprir escrupulosamente coas directrices marcadas pola nova normativa, actuando de modo efectivo,

***"As empresas e os gobernos deben percibir GDPR máis como unha vantaxe competitiva que como unha vía para simplemente evitar unha multa"***




coherente e seguro ante posibles ameazas que poidan afectar tanto á información corporativa como aos datos de clientes, so pena de afrontar sancións económicas -de 20 millóns de euros ou o 4% dos ingresos corporativos-, e inconmensurables repercusións indesexables en canto reputación.

## Orzamento TI ao alza

Unha enquisa en torno ao momento de GDPR, levada a cabo por IDC entre 250 empregados de empresas públicas e privadas en toda Europa, indica que o orzamento de TI para adaptar o cumprimento de GDPR continuará á alza. No caso concreto de España, prevese un incremento do 24% entre 2016 e 2021, estando fixado o orzamento de TI das empresas para adaptar a nova lexislación GDPR en140 millóns de euros en 2018 fronte aos 97,4 millóns de euros de 2017.

A pesar destas cifras, o camiño será arduo e longo

Volver ao sumario

porque só un 10% das empresas españolas consultadas asegura estar a cumprir xa a norma, mentres que outro 24% afirma acabar de decatarse de que é GDPR e un 4% recoñece abertamente non saber que é. Nun punto intermedio, atópase o 28% da mostra que valora GDPR como unha oportunidade para mellorar a eficiencia do goberno da información no seo da empresa.

Todo apunta a que as áreas que primeiro investirán para dar cumprimento á nova norma serán a xestión de identidades e o acceso da información (citado por 70% da mostra); aquelas que incorporen tecnoloxía que permita saber que aplicacións usan datos persoais (segundo expresa o 66% dos consultados en España), e a comunicación interna e formación dos empregados.

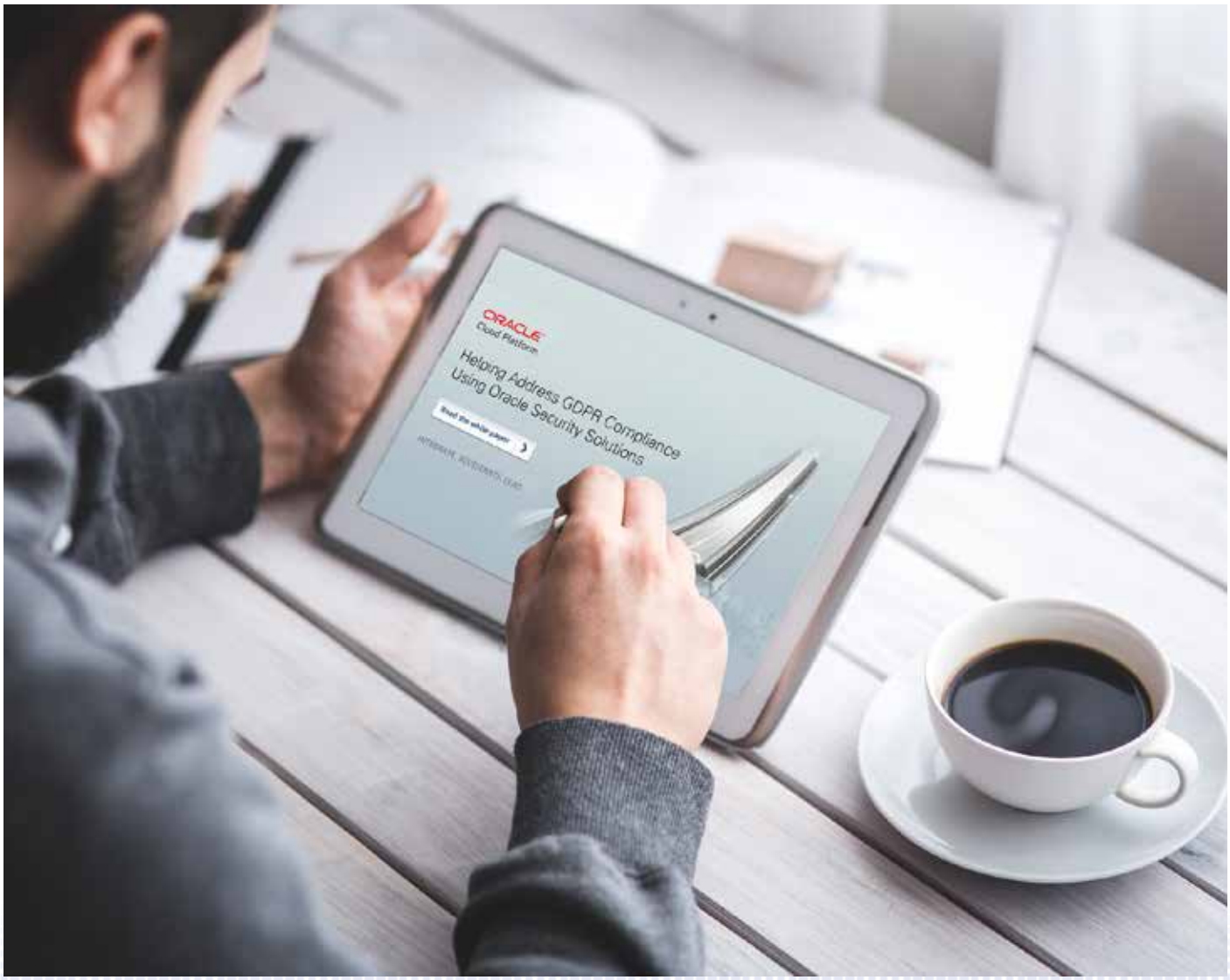
Por fin, a ciberseguridade elévase a rango de "requisito no deseño das arquitecturas TI". Seguridade no deseño e por defecto son conceptos que ata agora quedaban nos manuais e que grazas á obrigatoriedade deste regulamento, convértese nun principio reitor inescusable dos procesos e servizos de tecnoloxía que soportan ao negocio.

As empresas e os gobernos deben percibir GDPR máis como unha vantaxe competitiva que como unha vía para simplemente evitar unha multa. A uns meses da entrada en vigor da nova lexislación, é recomendable que expoñan xa un enfoque táctico que lles permita coñecer o punto no que están en canto a protección dos seus datos, de face a calibrar o risco latente. A partir de aí deberán designar a unha persoa que analice como se aplica a norma, e se é da man de expertos en consultoría e tecnoloxía, mellor porque estes son precisamente quen atesouran o coñecemento e os mecanismos capaces de permitir observar como se está adoptando na práctica.

***"GDPR será pedra angular de calquera proceso de negocio que interactúe co cliente final"***

E é que aquelas empresas que non cumpran con GDPR, non soamente van xogarse o seu prestixio como marca, senón que van quedar atrás no novo marco competitivo. O regulamento europeo, supón non só crear unha garantía fronte ao usuario final, senón tamén, demostrar que as empresas comprenderon que a transformación dixital supón garantir o éxito dos seus clientes: a confianza como base na dixitalización.

GDPR non será unha moda pasaxeira, está para quedar e sen dúbida, será pedra angular de calquera proceso de negocio que interactúe co cliente final.




Volver ao sumario

# Os ciberataques, unha ameaza real

Salvador Serrano
Responsable da Área LOPD de PSN Sercon

A seguridade é un aspecto crucial das nosas vidas, e o seu interese é maior canto máis importante sexa aquilo que queremos protexer. As nosas familias, os nosos países ou a nosa economía merecen os máis altos niveis de protección, e a sociedade desenvolveu instrumentos para proporcionala. As ameazas contra as que nos enfrontamos son, por desgraza, numerosas, e a estas, nas últimas décadas, engadiuse unha nova: os ciberataques, cuxo impacto é cada vez maior. Para facerlles fronte son necesarios novos instrumentos e novos recursos.

A tarefa non é, con todo, fácil. Son necesarios máis recursos pero, ante un escenario de constante avance tecnolóxico, tamén hai que saber como empregalos e mantelos constantemente actualizados. ***É necesario apoiarse nunha formación tecnolóxica e científica de calidade que prepare a persoas para combater aos exércitos de piratas informáticos que xa operan a gran escala ao servizo de organizacións criminais, e mesmo de estados***. É tamén necesario contar co compromiso das institucións para conceder a importancia que merece a ciberseguridade, e pór en marcha sistemas de seguridade adecuados. E, por suposto, é máis que nunca necesaria a colaboración entre países para facer fronte a unha ameaza que non coñece fronteiras e que se aproveita da crecente interconectividade de todos os aspectos das nosas vidas.

Casos recentes como o virus Wannacry, que afectou a 230.000 computadores en máis de 150 países incluíndo obxectivos de tanta relevancia estratéxica como Telefónica ou o sistema nacional de saúde británico, ou como o virus Petya, que bloqueou o xuño pasado os sistemas informáticos dunha boa parte do tecido empresarial de Ucraína afectando a bancos, xornais e compañías eléctricas son un recordatorio claro de que os ciberataques son unha ameaza real.

No que se refire ao sector sanitario en particular, destacan os numerosos casos de ransomware a hospitais en Estados Unidos nos que se pon en risco a atención a pacientes bloqueando os sistemas informáticos. As consecuencias dun ataque informático a un hospital son especialmente graves, dada a importancia do que hai en xogo: a vida dos pacientes e a integridade dos datos persoais sanitarios.

A Axencia Europea de Seguridade das Redes e da Información publicou un estudo recentemente sobre as principais ameazas que afrontan os hospitais intelixentes. O estudo destaca o malware como o principal factor de risco, e advirte de que cada novo dispositivo conectado é un obxectivo potencial para un ataque.

> ***"É necesario apoiarse nunha formación tecnolóxica e científica de calidade que prepare a persoas para combater aos exércitos de piratas informáticos que xa operan a gran escala ao servizo de organizacións criminais, e mesmo de estados"***

Outras modalidades de ciberataque, como os intentos de manipulación electoral por terceiros países en diversos procesos electorais, son un recordatorio de como este tipo de ataques poden adoptar moitas formas e métodos. Ás veces nin tan sequera é necesaria unha gran sofisticación senón un simple descoido. Un rudimentario ataque de phishing, por exemplo, levou á revelación dun gran número de correos privados da candidata demócrata á presidencia, Hillary Clinton, que ben puideron custarlle as eleccións.

Segundo un recente estudo da firma de software de seguridade Kaspersky, máis do 50 % das empresas sofren polo menos un ciberataque ao ano, mentres que só o 48 % delas pensan que vaian sufrir algún e que deberían prepararse para eles. Isto supón unha disociación entre a percepción da ameaza e a súa realidade que non nos debe pasar desapercibida.

Este dato revelador -unido aos numerosos casos

Volver ao sumario

recentes de ciberataque- reforza o convencemento de PSN sobre unha necesaria aproximación estratéxica cara á ciberseguridade. Non basta con reaccionar ante os ataques e tentar minimizar as súas consecuencias, senón que necesitamos construír unha cultura na que a ciberseguridade sexa un alicerce fundamental. Isto axudaranos a ir un paso por diante dos cibercriminais, a mantelos baixo control e, ademais, a desenvolver unha vantaxe competitiva tanto a nivel empresarial como institucional.

Non é difícil imaxinar un futuro no que os cibercriminais tenten golpear sectores estratéxicos das nosas economías como a rede eléctrica ou o tráfico aéreo. Os países e empresas que optasen por prepararse e tomarse en serio as ameazas serán os mellores situados para facerlles fronte, e tamén os que poderán seguir operando mentres outros se vexan obrigados a paralizar a súa actividade. Á ciberseguridade podémola converter en oportunidade, se nos dedicamos a ela coa eficiencia e os recursos necesarios.

A tentación, ante as ameazas que emanan das novas tecnoloxías, podería ser darlles as costas. Pero iso non é unha opción. A solución non é volver atrás senón ir cara adiante, aínda que, iso si, sempre sabendo o terreo que pisamos.

No terreo médico, sen ir máis lonxe, as posibilidades que proporcionan as novas tecnoloxías son enormes. Pero en

***"Un recente estudo do Pew Research Center colocou aos ciberataques como a terceira causa de preocupación ao redor do mundo"***

ningún caso debemos deixar de lado que todo aparello conectado é susceptible de ser atacado de maneira remota e que, cando temos vidas humanas entre mans, debemos prestar unha atención especial á seguridade.

Por último, gustaríame mencionar ***un recente estudo do Pew Research Center***, un dos centros de estudos sociais máis importantes de Estados Unidos, que ***colocou aos ciberataques como a terceira causa de preocupación ao redor do mundo***, tan só superada polo ISIS e o cambio climático. Este estudo pon de manifesto que a gravidade desta nova ameaza xa está a ser percibida claramente pola sociedade e que se demandan, cada vez máis, medidas para combater aos cibercriminais.

O futuro xa está aquí e converteuse en presente. De nós depende non quedarnos atrás e estar á altura do desafío que supón adaptarse a unha contorna tecnicamente moi complexo e en constante cambio. Non é fácil, pero diso depende, sempre máis, a nosa seguridade, a nosa estabilidade e o noso benestar.

Volver ao sumario

# Ciberseguridade nas empresas do século XXI

Susana Rey
Responsable de Seguridade de R

A dixitalización, a industria 4.0, a Internet das Cousas (IoT)… É imprescindible que nos situemos na nova contorna tecnolóxica para falar de ciberseguridade. E do mesmo xeito cómpre ter presentes os novos riscos que nos perseguen: *hackers* profesionais que forman parte de organizacións delituosas perfectamente organizadas (mesmo dirixidas polos gobernos dalgúns países) ou *ciberhacktivismo*, entre outras ameazas.

Tamén é de recibo fornecer de datos estatísticos e información sobre as inxentes perdas das empresas por mor de ciberataques e inclusive porcentaxes de empresas afectadas. A importancia do tema xa ninguén a cuestiona, sobre todo dun tempo ata a data, pois temos exemplos varios de incidentes graves con repercusións mediáticas que veñen de poñer as vítimas na palestra pública pola mala xestión da súa seguridade (*Wannacry*, *Petya*, caso *Equifax*…).

Hai que concienciar -e moito aínda- tanto á empresa como á sociedade, da importancia da ciberseguridade, de que os riscos asociados a non fomentala son reais e poden rematar ocasionando graves repercusións nas nosas vidas, laborais e privadas. Sen embargo, o esencial non é tanto falar da problemática – que tamén- coma do que debemos e podemos facer as empresas da nova era para xestionar esta situación e saír ben paradas.

## Cambio de mentalidade

As culturas e xeitos de facer das corporacións están cambiando, por fortuna. Chegou o momento de romper coas ideas predeterminadas que condicionan a toma das mellores decisións das empresas neste eido. O primeiro é aceptar que calquera empresa, independentemente do seu tamaño, situación xeográfica, sector… é obxectivo potencial de ciberataques. E tamén calquera cidadán. Isto redunda, loxicamente, en riscos para as empresas, posto que o dispositivo infectado (pc ou *smartphone*) será tamén moi probablemente empregado no contorno laboral. E xa non falamos só de pcs: *smartphones*, routers, cámaras de videovixilancia, teles intelixentes... e moi pronto tamén ata as nosas neveiras deberán ser protexidas. É tempo de desbotar a idea de que o noso negocio non necesita protección. Todos temos que coidar da nosa seguridade.

O segundo cambio consiste en aceptar que a seguridade absoluta non existe. Por moito que traballemos ou que invistamos, sempre quedará algunha fenda que, unida a cibercriminais, traballadores maliciosos ou a simples erros humanos, poden poñer en xaque a ciberseguridade da empresa. Por iso hai que estar preparados para detectar, respostar e recuperarse tras unha falla nesta área, porque sempre cabe a posibilidade de que se produza.

Isto non quere dicir que non poidamos facer nada; nin moito menos. Sempre seremos obxectivos e sempre será posible que os atacantes poidan lograr os seus fins pero o importante é reforzar a seguridade no lugar axeitado dos procesos empresariais, para asegurar que, pase o que pase, imos ser quen de recuperarnos co menor custo posible.

## Xestión de riscos, tecnoloxía e colaboración

E como o logramos? O certo é que non hai recetas máxicas porque cada organización é diferente e debe buscar o seu xeito particular de facer as cousas.

Pero si se poden avanzar tres ideas básicas:

**Xestión de riscos**. Como ninguén ten infinitos recursos para gastar en ciberseguridade, debemos investir o dispoñible intelixentemente. Todas as organizacións fan, dun xeito máis informal ou dentro dalgún modelo estandarizado, xestión de riscos empresariais. Pero normalmente evalúanse e trátanse os relativos ao negocio é ás finanzas, e son unicamente estes os que se teñen en conta á hora de tomar as decisións empresariais. Nestes momentos é imprescindible engadir a esta xestión os riscos relacionados cos ciberataques e as consecuencias que poderían ter para o negocio; e sempe dentro do modelo xeral que xa existe na organización, non como algo aillado ou diferente. Nos últimos anos estase a ver, en organizacións máis maduras na xestión da ciberseguridade, como os responsables de seguridade

***"Sería un grande erro pensar que a ciberseguridade é unha cuestión puramente tecnolóxica"***

Volver ao sumario

*"o grande reto que ten a ciberseguridade hoxe en día é o de dispor dun modelo de xestión eficiente, intelixente e colaborativo"*

están evolucionando dende postos puramente técnicos a postos de xestión de riscos, nos que se traballa moi preto dos responsables financiero ou de "compliance" da compañía. Evolución que os profesionáis das telecomunicacións podemos e debemos impulsar para lle dar máis visibilidade e eficiencia á xestión da ciberseguridade.

**A tecnoloxía**. Sería un grande erro pensar que a ciberseguridade é unha cuestión puramente tecnolóxica. A tecnoloxía é necesaria, imprescindible: *firewalls*, antivirus, ferramentas anti-DDoS, balanceadores, IDS/IPS, SIEMs… e poderiamos seguir engadindo tecnoloxías para a seguridade que son necesarias, nalgúns casos imprescindibles. Pero por si soas non terían sentido porque, como dicían nalquel anuncio: "a potencia sen control non serve de nada". A ciberseguridade é algo moito máis complexo e debe ir máis aló das áreas técnicas da compañía: xestión de persoas, formación e concienciación, organización interna, procedementos, lexislación, intelixencia, comunicación… Todo isto debe ser xestionado e coordinado, ademais de avalado por un amplo coñecemento técnico. Cada vez vai ser máis necesario contar con persoal con coñecementos técnicos sólidos en todas esas áreas das compañías. Sen dúbida, tamén se trata dunha grande oportunidade para a nosa profesión.

**A complexidade**. Nun mundo tan tecnolóxico e complexo, no que cada vez temos máis sistemas interconectados, novos ecosistemas (industria 4.0, IoT…) e no que cada vez se evoluciona máis rápido, a seguridade ten o mesmo nivel de complexidade e de cambio constante. Isto conleva que a meirande parte das empresas non poidan dispoñer de áreas de ciberseguridade con presenza de profesionais preparados en todos os eidos implicados. Nin as compañías que máis invisten nestes servizos son quen de coñecer todo o que está a acontecer ao longo do mundo.

Fronte a isto a única solución posible é a da **colaboración**, tanto entre organizacións privadas como entre o sector público e o privado. Colaboración que se pode entender como a busca de socios que lles permitan ás empresas dotarse de áreas de ciberseguridade con recursos humanos e coñecementos dabondo a costes axeitados. O desenvolvemento de MSSP (Security Service Providers), como evolución dos SOCs e o persoal coas ferramentas e experiencia precisas ao dispor de todos vai ser básico nos próximos anos. E colaboración entendida como as redes de intercambio de información temperá que nos permiten coñecer o que lles está pasando a outros, para nos defender antes. Organismos públicos como Incibe ou o CCN-Cert, ou Certs privados dentro dos mesmos MSSPs poden axudarnos a todas as organizacións a participar nestas redes e recibir e achegar coñecemento para a seguridade de todos.

Dende esta perspectiva, o grande reto que ten a ciberseguridade hoxe en día, e na que os Enxeñeiros de Telecomunicación e o sector das telecomunicacións temos moito que aportar, é o de dispor dun modelo de xestión eficiente, intelixente e colaborativo, que nos leve a facer máis con menos e que nos permita, a organizacións e sociedade, acadar o nivel de seguridade co que cada un se sinta cómodo.


Volver ao sumario

# A Ciberseguridade e outros camiños do ensino na Escola de Enxeñaría de Telecomunicación de mañá

Iñigo Cuiñas
Catedrático de Universidade.
Director da Escola de Enxeñaría de Telecomunicación. Universidade de Vigo

teleco.uvigo.es

A profesión da Enxeñaría de Telecomunicación atópase na disxuntiva das súas miras futuras, e con ela (ou canda ela, ou quizabes por diante dela) as Escolas nas que preparamos aos enxeñeiros e enxeñeiras de mañá. A demanda de profesionais TIC crece moito máis que a vocación entre os xoves de estudar estes estudos ou, en xeral, estudos do ámbito STEM (Ciencias, Tecnoloxías, Enxeñarías e Matemáticas). Podemos pensar que se dan dúas complexidades para acceder á formación no eido da Enxeñaría de Telecomunicación, pero tamén para saír das Escolas ao mundo laboral.

Dáse a situación paradóxica de que segundo a Sociedade do Coñecemento avanza, e con ela as moitísimas aplicacións desenvolvidas no eido das TIC en xeral, e das Telecomunicacións en particular, acadando máis e máis sectores produtivos, a propia profesión que lidera estes desenvolvementos estase a diluír nunha "desidentificación". As TIC están a acadar unha transversalidade tal que nestes intres non é doado explicar, a un rapaz novo, a que vaise dedicar un profesional da Enxeñería de Telecomunicación dentro de cinco anos. E isto limita o atractivo das Escolas de Enxeñaría de Telecomunicación para os novos alumnos. A clara identificación cos sistemas de comunicacións e coas redes que tiñamos os telecos hai vinte anos xa non é tal, e os nosos titulados traballan en empresas tipicamente de telecomunicación, pero tamén en outros sectores que hai anos eran cotos pechados só para enxeñeiros industriais, ou para economistas, ou para científicos.

Esta é unha situación moi positiva para quen xa ten as competencias profesionais, xa que o seu horizonte laboral crece con respecto ao máis sectorizado de anos atrás. Pola contra, non resulta tan doada a captación de novos talentos para formarse nas nosas tecnoloxías, xa que non teñen a identificación da profesión que outros, máis vellos, tiñamos. Aquel presente-futuro tecnolóxico que imaxinabamos, coa explosión da telefonía móbil e a Internet, chegou. E chegou para ficar connosco! Mais agora eses avances están tan imbricados na sociedade que se converteron na neveira da nosa infancia: se sempre houbo neveira na casa, non miramos a neveira como un avance tecnolóxico, non pensamos na Enxeñaría que hai dentro dela... simplemente está e funciona. As xeracións novas non miran aos móbiles á Internet como avances tecnolóxicos... simplemente están e funcionan (coma a nosa neveira!). E non se decatan da Enxeñaría que hai detrás, que fai que nos comuniquemos cando e como queramos.

***"Aquel presente-futuro tecnolóxico que imaxinabamos, coa explosión da telefonía móbil e a Internet, chegou"***

Por outra banda, o crecemento económico e de benestar tamén move o foco do prestixio social da Enxeñaría. Nas etapas de desenvolvemento dos países, a Enxeñaría mírase como o motor deste desenvolvemento, xa que é quen de impulsar un cambio económico ou ata social, como vemos nos últimos anos. Unha vez que a sociedade acada un grao importante de desenvolvemento e benestar, o prestixio (e o diñeiro!) trasládase ao mundo financeiro e emprendedor. É un fenómeno que se deu hai décadas en Estados Unidos ou no Reino Unido, sociedades que se desenvolveron antes que a nosa, e onde o número de profesores e investigadores, e non digamos estudantes, de Enxeñaría de orixe local baixa ano a ano mentres medran os que veñen doutras áreas (Sudeste Asiático, América Latina, ou Medio Oriente e India no caso británico) nas que un enxeñeiro ou unha enxeñeira conserva ese prestixio social que foi caendo entre os locais. Tamén ocorre en Europa Central, inda que máis recentemente: moitos dos estudantes de doutoramento en Alemaña, Bélxica, Holanda, etc. non son do propio país senón que veñen de economías menos desenvolvidas. Dalgún xeito é un dano colateral do progreso económico e social.

Temos, pois, unha situación na que a captación de novos talentos nas Escolas de Enxeñaría vese limitada pola indefinición da propia Enxeñaría de Telecomunicación, que non se identifica facilmente cunha actividade profesional, e pola diminución no prestixio social da profesión. E, por outra banda, as carreiras laborais dos titulados en Telecomunicacións os levan a requirir

Volver ao sumario

unha formación adicional, especializada en temas moi concretos, que ten que vir apoiada nos coñecementos xeralistas que fan do profesional un enxeñeiro de Telecomunicación. Isto pon ao graduado na dúbida de difícil solución entre unha formación que o leve cara a Enxeñaría de Telecomunicación clásica ou outra que o apunte cara a unha destas profesións emerxentes tan demandadas na actualidade. A co graduado ou graduada, as propias Escolas estanmos na mesma dúbida de imposible solución.

As Escolas de Enxeñaría de Telecomunicación non queremos (ou non debemos?) renunciar a ofertar aos nosos graduados a posibilidade de cursar unha titulación de máster en Enxeñaría de Telecomunicación que lles equipare aos enxeñeiros de Telecomunicación das xeracións anteriores: unha formación ampla, que cubra ou complemente as diferentes ramas da nosa profesión (se é que esta profesión pode limitarse aos Sistemas de Telecomunicación, Telemática, Son e Imaxe, e Electrónica na que tradicionalmente estamos encaixados, pero este é outro debate). E que cumpra cos corsés establecidos no Real Decreto que define as competencias do máster se vai proporcionar atribucións profesionais. E este empeño en manter a preparación de novos telecos precisa dun apoio por parte das organizacións profesionais e das propias empresas: se o que demandan é enxeñeiros de Telecomunicación clásicos, estes son os titulados do Máster en Enxeñaría de Telecomunicación. Se o tecido empresarial non explicita esta demanda vai ser moi difícil seguir a sacar ao mercado estes titulados sendo eficientes en relación co custo da propia titulación.

A competencia en termos de formación a temos na propia casa. Hai novas profesións relacionadas coas TIC que demandan tamén formación a nivel máster. É o caso da Ciberseguridade. Nestes casos, as sinerxias coas outras profesións relacionadas, como é a Informática, son imprescindibles para que a formación dos profesionais sexa completa e tamén para garantir unha eficiencia nestas titulacións que facilite a súa continuidade. No caso galego, a Escola de Enxeñaría de Telecomunicación da Universidade de Vigo e a Facultade de Informática

***"Hai novas profesións relacionadas coas TIC que demandan tamén formación a nivel máster. É o caso da Ciberseguridade"***

da Universidade da Coruña fomos quen de converxer nunha titulación única, interuniversitaria, de Máster en Ciberseguridade que verá a súa posta de gala no próximo curso 2018/19. O traballo de coordinar dous centros universitarios e dúas profesións con características diferentes, como son a Enxeñaría de Telecomunicación e a Informática, estará ben invertido cando saian ao mercado laboral os primeiros titulados e vexamos unha resposta positiva por parte do tecido empresarial e institucional galegos.

Como paso previo, na Escola de Teleco de Vigo levamos dous anos a impartir un curso de "Introdución á Ciberseguridade" co apoio decidido de R e de pequenas empresas do sector galego. O curso, impartido por profesionais en activo (tanto telecos como informáticos) está a ser un éxito de demanda. Ademais, a comezos de ano creouse a Cátedra Deloitte de Ciberseguridade na Universidade de Vigo, cuxo Reitor honroume coa dirección. Dende ela tentaremos impulsar iniciativas de formación e difusión desta profesión emerxente.

E nesas estamos na Escola de Enxeñaría de Telecomunicación, buscando xeitos de facer chegar aos máis novos o que representa a nosa profesión nunha sociedade tecnolóxica como a que vivimos (para o que a axuda de tódolos compañeiros de profesión é, máis que ben recibida, reclamada) y propoñendo saídas formativas aos nosos graduados: que sexan quen de decidir emprender a súa vida laboral cun título que os capacita para elo (con atribucións de Enxeñaría Técnica de Telecomunicación) ou de acadar máis formación no eido das Telecomunicacións clásicas ou en profesións novas, como a que propoñemos en Ciberseguridade. A demanda do mercado é quen decidirá o futuro destas propostas.

Volver ao sumario

# Telefónica e a súa estratexia de ciberseguridade global

Marta Menéndez
Directora de Telefónica en Galicia

As crises de seguridade na Rede vividas durante o último ano, co seu reflexo crítico no funcionamento de infraestruturas craves como hospitais ou aeroportos, puxeron de manifesto máis que nunca a necesidade de que as empresas, as institucións e os gobernos dótense de estratexias e sistemas de ciberseguridade sólidos, aínda entendendo que en ciberseguridade, como en calquera forma de ameaza, non existe o cento por cento de protección.

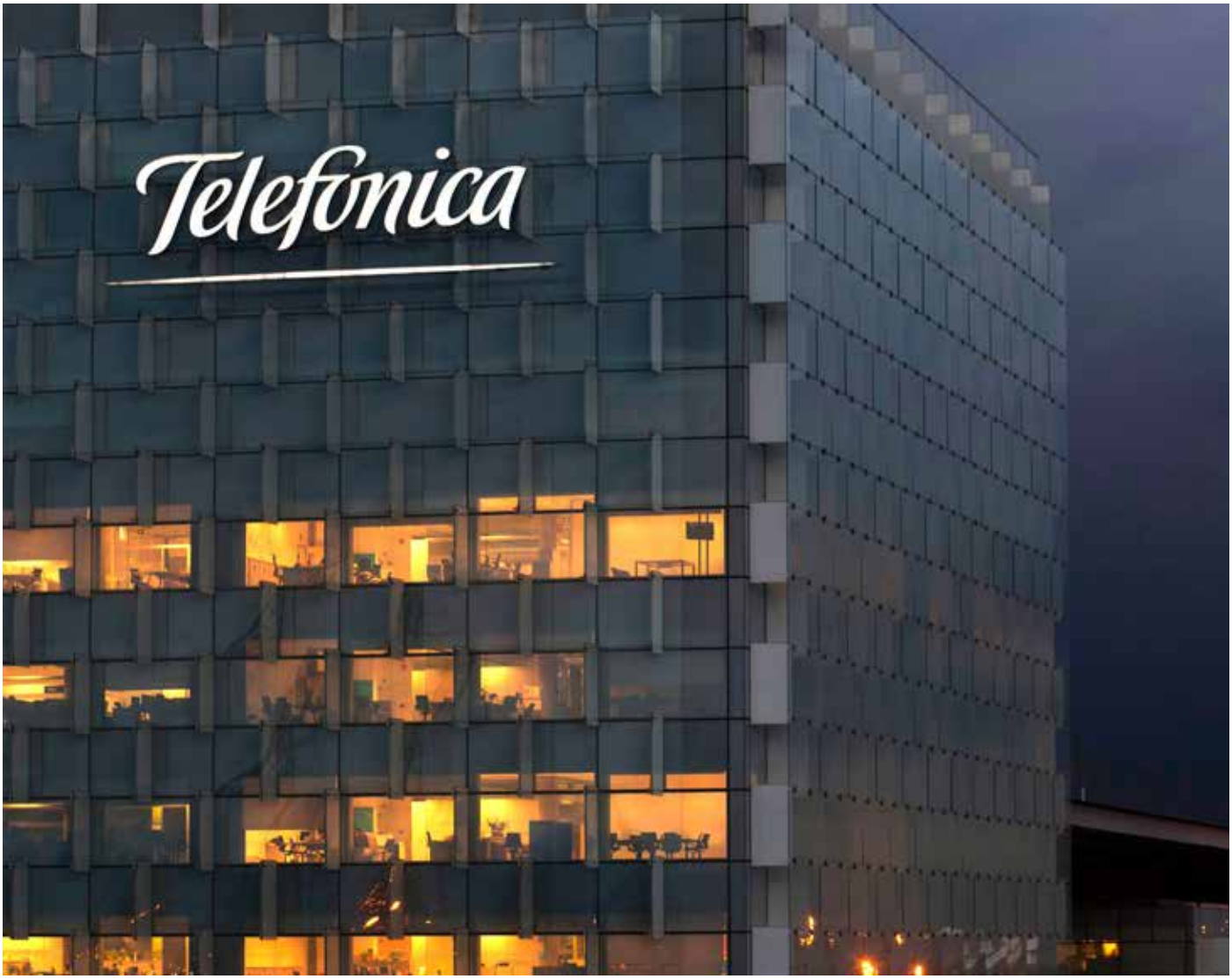
Telefónica leva moitos anos dotando aos seus clientes dunha estrutura de tecnoloxías, procesos e equipos humanos preparados para xestionar a ciberseguridade do

***"En ciberseguridade, como en calquera forma de ameaza, non existe o cento por cento de protección"***

día a día, e para dar unha resposta rápida e centralizada a calquera ataque. Trátase dunha rede de seguridade global con 8 centros físicos os -SOCs ou Security Operation Center- en Estados Unidos, México, Colombia, Perú, Chile, Brasil, Arxentina e Turquía, e o Centro de Operacións de Seguridade Global de Madrid.

Telefónica, ademais, colabora con socios de referencia

Volver ao sumario




no ámbito da seguridade global, como Intel Security, Symantec, Paloalto ou Logtrust, entre outros, o que nos permite configurar uns servizos do máis alto nivel en ámbitos como a instalación de infraestruturas, a vixilancia dixital, a xestión de vulnerabilidades, o antifraude, os anti DDos (protección ante denegación de servizos distribuídos, que poden afectar á dispoñibilidade de activos das empresas), navegación segura, protección dos correos electrónicos ou todo o ámbito da identidade, como a certificación SSL, firma biométrica, mobile connect, etc.

En definitiva, a ciberseguridade será -éo xa, de feito- un factor clave para a estabilidade da economía mundial, e para as empresas de calquera tamaño, polo que máis que puros resellers de software, que cubran só aspectos parciais da ciberprotección, necesítanse compañías e servizos integrados como os de Telefónica, nos que, volvendo ao comezo deste artigo, a combinación de infraestruturas físicas, procesos e equipos humanos altamente especializados, e unha estratexia global clara, poderán dar unha resposta adecuada a esta ameaza.

***"A ciberseguridade será -éo xa, de feito- un factor clave para a estabilidade da economía mundial"***

Volver ao sumario

# A ciberseguridade como a chave para o futuro

Javier Augusto González
Project Manager do Departamento de I+D de TELEVES

Televes

Nos últimos tempos é frecuente escoitar o termo ciberseguridade en múltiples contextos, incluído nos medios de información máis xerais, grazas a episodios coma o sufrido co ataque dun ransomware a nivel global durante este ano 2017 e á tendencia crecente do número de ciberataques a todos os niveis. Sen embargo, a pesares do estendido do seu uso e da crecente preocupación demostrada polas entidades gobernamentais (coma demostra o anuncio da creación dunha axencia específica europea de ciberseguridade por parte do presidente Juncker neste setembro), é un concepto que aínda está infravalorado para a meirande parte da sociedade debido, en gran medida á dificultade para esbozar a súa importancia.

Poñamos certos símiles que nos permitan contextualizar a importancia deste ámbito: ¿vivirías nunha casa completamente de cristal, na que todo o que ocorrese no seu interior fose visible dende o exterior? ¿Deixarías instalar na túa casa ou negocio micrófonos que puidesen ser escoitados por calquera (incluso a túa competencia)? ¿Deixaríaslle a túa tarxeta de crédito e a túa clave persoal a alguén en quen non confiases? As respostas a estas preguntas  poden parecer obvias, pero cando se trata do mundo dixital, non todo o mundo e consciente de que as súas decisións poden ser equivalentes a dar unha resposta afirmativa a algunha desas cuestións. No contexto da transformación dixital que estamos a vivir, camiño de crear una imaxe dixital e aumentada da realidade grazas a tecnoloxías como o Internet das Cousas ou a Realidade Virtual, a ciberseguridade é un factor habilitador clave para poder alcanzar o verdadeiro potencial desta nova revolución social e industrial. A ciberseguridade permite garantir aspectos coma a integridade, a protección ou a privacidade dos datos, así como asegurar a dispoñibilidade do servizo (clave para moitas aplicacións), xerando deste xeito a confianza necesaria no usuario consumidor que permita alcanzar esa imaxe de futuro.

***"É clave explotar as sinerxias que as novas tecnoloxías están creando para conseguir solucións de ciberseguridade de última xeración adaptadas aos novos retos"***


*Televes coordina o proxecto europeo H2020 GHOST no eido da ciberseguridade no fogar (GA. 740923 )*

Segundo o, o Internet das Cousas é unha das tecnoloxías disruptoras de referencia nesta transformación dixital, baseándose no concepto de hiper-conectividade para todos os elementos físicos presentes no mundo real. Deste xeito, todos os elementos dentro, por exemplo, dunha casa ou dunha fábrica xeran, reciben e transmiten información dende e cara a repositorios na nube, permitindo a virtualización dos procesos físicos (dende a xestión da saúde, ata a fabricación, pasando pola automatización dunha vivenda, procesos de compra, etc.). Dun xeito simplificado, é necesaria a instalación de dispositivos (tanto sensores como actuadores) con capacidade de comunicación no entorno escollido, tendo en conta que os devanditos dispositivos contarán con limitada capacidade de memoria, procesamento e autonomía. Polo tanto, os conceptos de security-by-design e privacy-by-design cobran especial relevancia no deseño destes elementos constituíntes, así como os sistemas de monitorización e detección de posibles ameazas ou ataques. É necesario dispor de dispositivos e sistemas con capacidade para

Volver ao sumario


protexerse a sí mesmos e á información que xeran e consumen de cara a garantir que esa imaxe virtual do mundo se corresponde coa realidade, e que os servicios baseados na mesma funcionan conforme ao esperado.

Outro dos campos que máis interese espertou nos últimos anos é o concepto de análise e minería de datos. Ligado ao Internet das Cousas (que xera un enorme conxunto de datos conectados co mundo real), a análise masiva de datos baséase en dispor dunha elevada cantidade de información e procesala de xeito que se poidan extraer relacións entre as diversas variables presentes, así como controlar e monitorear a evolución temporal das variables de cara a conseguir optimizar e mellorar os procesos asociados á devandita información analizada (por exemplo, controlar de xeito autónomo a evolución médica dunha persoa ou optimizar o proceso produtivo dunha cadea de montaxe). Sen embargo, estas ferramentas non teñen sentido se os datos que empregan non son correctos (debido a un ataque que cambie a información xerada ou xere nova información) ou non están dispoñibles (debido a posibles ataques de denegación de servicio), entre outros.

Ademais, as tecnoloxías previamente introducidas están claramente ligadas coa importancia e relevancia da propiedade dos datos e da información, especialmente nos casos relativos ao tratamento de datos persoais. É totalmente necesario dispor de sistemas e solucións que garantan que a propiedade dos datos non é violada ao longo da súa cadea de uso, que están claramente protexidos fronte a accesos externos, e que son tratados con total transparencia de acordo as regulacións vixentes.

Estes son dous exemplos da importancia da ciberseguridade como chave para o desenvolvemento das tecnoloxías que marcarán esta nova época dixital. Curiosamente, estas mesmas tecnoloxías pódense converter nun aliado excepcional para crear solucións de ciberseguridade novidosas e efectivas. Por exemplo, o uso de técnicas de análise masivo de datos ou de minería de datos pode axudarnos a detectar patróns sospeitosos no comportamento dun dispositivo dentro dunha instalación, ou o uso de técnicas de blockchain pode garantir que a información contida nun sistema de datos é correcta grazas a a colaboración entre os distintos nodos da cadea. Así pois, é clave explotar as sinerxias que as

***"Temos a responsabilidade social de crear novas solucións de ciberseguridade que permitan xerar a confianza necesaria nos diversos sistemas por parte dos usuarios finais"***

novas tecnoloxías están creando para conseguir solucións de ciberseguridade de última xeración adaptadas aos novos retos que se plantexan neste eido. Doutro bando, a democratización tecnolóxica asociada a este proceso de transformación dixital e a extensión da tecnoloxía a todos os ámbitos e mercados (do que son exemplo empresas como Alphabet, Amazon ou Uber) demandan que as solucións de seguridade deixen de estar centradas nos profesionais e teñan como obxectivo o propio usuario???, sen coñecementos avanzados de seguridade. A época na que as empresas de comunicacións e os gobernos eran as únicas entidades preocupadas pola integridade e seguridade da información xa pasou a a historia. É xa nestes intres o propio usuario ou propietario da información o que debe poder decidir como trata os seus datos e avaliar a seguridade dos mesmos.

Deste xeito, dende o sector ao que representamos temos a responsabilidade social de crear novas solucións de ciberseguridade que permitan xerar a confianza necesaria nos diversos sistemas por parte dos usuarios finais (persoas, institucións ou empresas indistintamente), baseándonos para elo na necesidade de aproveitar o coñecementos previos dos que dispomos. Este será un requisito indispensable para poder desencadear e soportar a evolución tecnolóxica asociada á transformación dixital na que xa estamos inmersos. Televés, como un dos actores implicados nesta transformación dixital, é consciente da importancia da ciberseguridade para esta nova etapa tecnolóxica e está a abordar este tema desde dúas ópticas principais: garantindo a integridade dos equipos e sistemas deseñados e creando solucións específicas de ciberseguridade que permitan ao usuario final sentirse cómodo e confiado co uso dos seus produtos.

Volver ao sumario

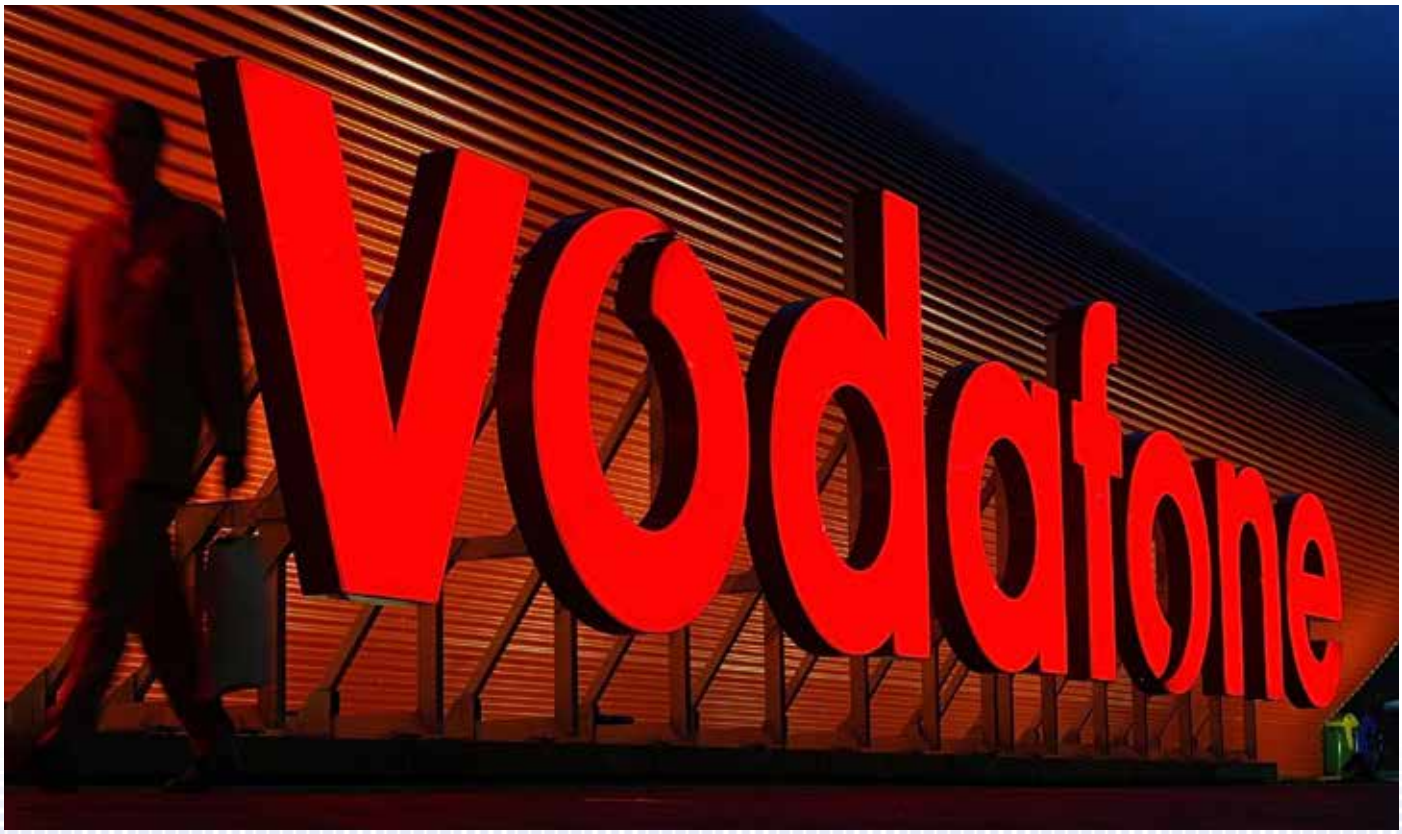
# A Seguridade na Internet das Cousas como premisa

Fran Vallejo
Director de Empresas Vodafone en Galicia

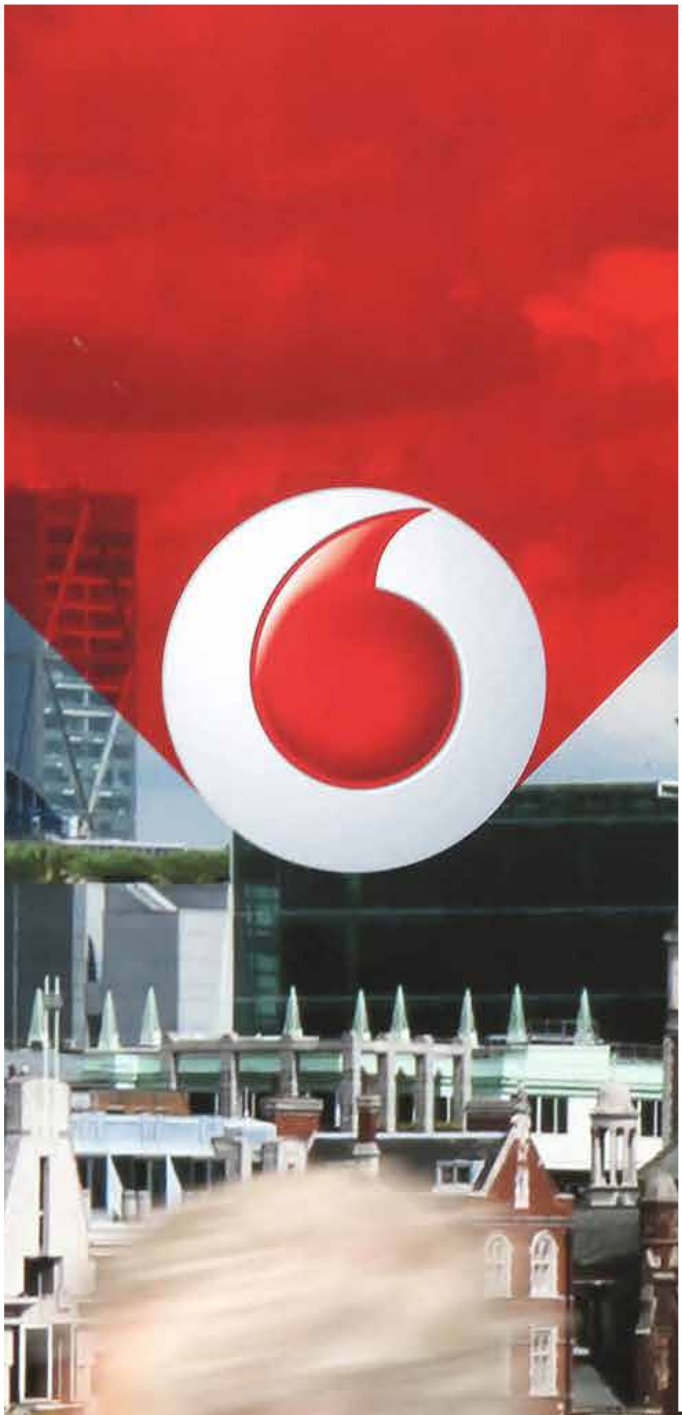
O avance da denominado Internet das Cousas posibilitará un mundo realmente conectado e atenderá as demandas de cidadáns e organizacións. Este concepto transforma todo tipo de activos en obxectos intelixentes, desde os accesorios máis pequenos como reloxos e outros dispositivos de consumo, ata vehículos e instalacións industriais de grandes dimensións. Neste sentido, xa son realidade, por exemplo, os beneficios da rede NB-IoT (Banda Estreita de Internet das Cousas) que permite conectar estes dispositivos entre si, mellorando o seu consumo de enerxía e a eficiencia do espectro en zonas de pouca cobertura, baixo terra ou en lugares de difícil acceso. Así, actualmente, cada vez máis empresas e administracións públicas españolas están a conectar os seus dispositivos a rede de Vodafone de NB-IoT, e creando solucións para cidades intelixentes en áreas como a Saúde, a Industria, a Agricultura ou a Automoción.

***"O 18% das empresas considera que as brechas de seguridade supoñen unha barreira potencial para a adopción da Internet das Cousas na súa organización"***

A seguridade debe ser unha parte intrínseca en todo este proceso, de modo que non constitúa unha preocupación para organizacións e administracións públicas no que respecta á implantación da Internet das Cousas. E é que, segundo sinala un estudo de Vodafone realizado en 2016, o 18% das empresas considera que as brechas de seguridade supoñen unha barreira potencial para a




Volver ao sumario



## *"A nosa solución Vodafone Secure Net conseguiu evitar máis de 196 millóns de ameazas de malware en 2016"*

adopción da Internet das Cousas na súa organización e un 30% recoñece que chegou a modificar os seus proxectos iniciais neste ámbito para evitar posibles riscos.

Se nos referimos especificamente ao noso país, a ciberseguridade, desde un ámbito máis amplo e non só aplicada a Internet das Cousas, é un tema prioritario. Así, o 86% dos negocios españois prevé aumentar o seu orzamento de ciberseguridade no próximos tres anos, mentres que o 91% afirma que a ciberseguridade mellorará a fidelización dos seus clientes.

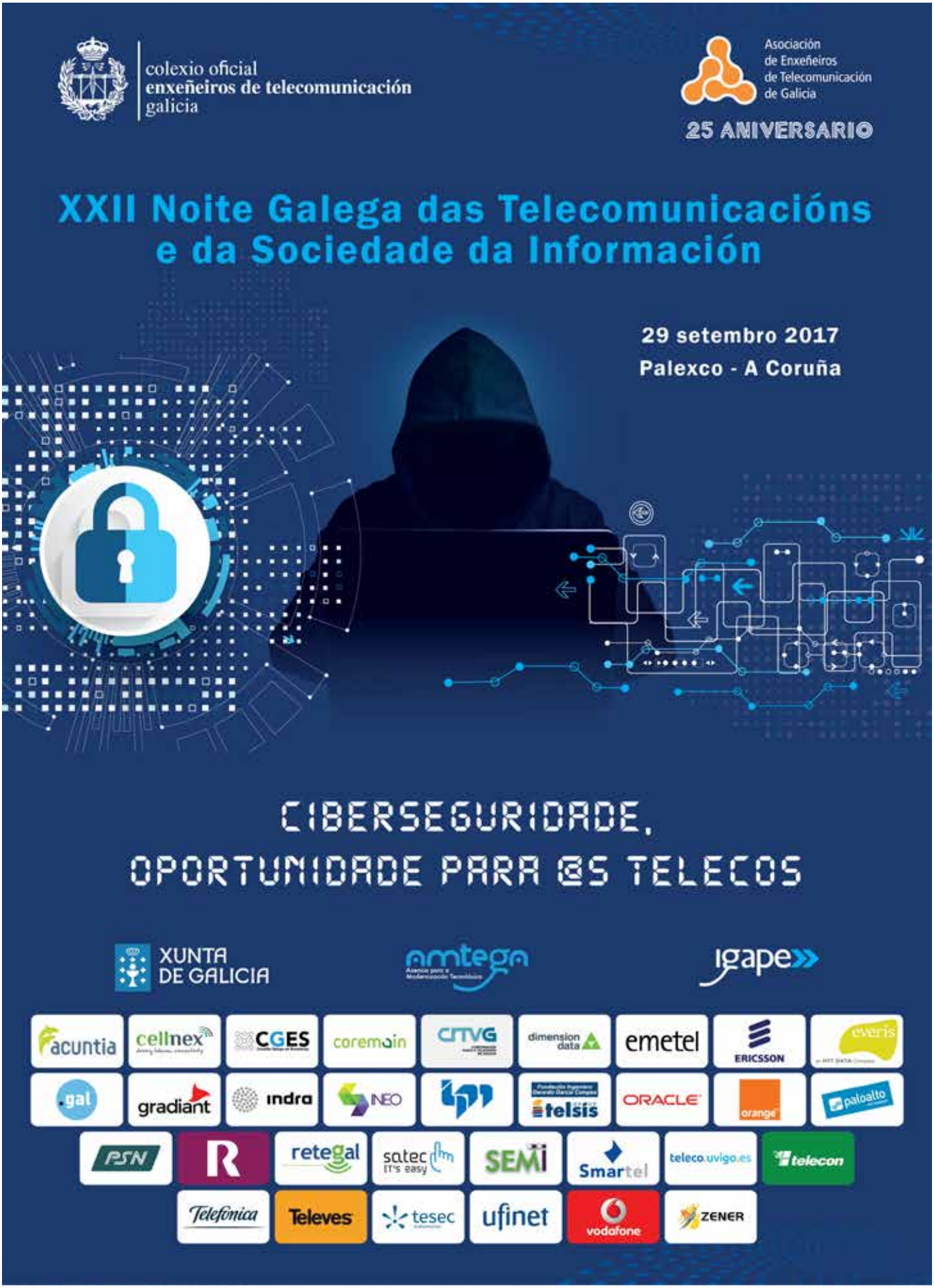
A seguridade é, por tanto, un dos principais factores que permiten o desenvolvemento e a adopción de novas solucións tecnolóxicas. Sen ir máis lonxe, o valor comercial das aplicacións de Internet das Cousas reside nos datos que recompila, que en moitas ocasións son datos críticos e cunha gran escalabilidade.

Desde Vodafone axudamos ás organizacións a protexer os seus datos contra roubos ou manipulacións, a través da propia SIM, no dispositivo, ou a través das redes e a plataforma central de xestión onde se aloxan estes datos. Ademais, ofrecemos a opción de aloxamento nunha nube privada para unha maior seguridade e mesmo solucións moi específicas vinculadas aos nosos centros de datos e os das empresas.

En Vodafone temos unha visión holística dos riscos aos que se enfronta a protección dos datos e traballamos continuamente para minimizar os riscos. Sen ir máis lonxe, a nosa solución Vodafone Secure Net conseguiu evitar máis de 196 millóns de ameazas de malware en 2016, o que supón unha media duns 46 ataques por cada cliente.

A innovación impregna todo aquilo que facemos e seguiremos traballando día a día para ofrecer as mellores solucións de conectividade e seguridade para todo tipo de organizacións.

Volver ao sumario




Volver ao sumario

## Co agradecemento do Colexio Oficial e da Asociación de Enxeñeiros de Telecomunicación de Galicia aos patrocinadores da XXII Noite Galega das Telecomunicacións e da Sociedade da Información

XUNTA DE GALICIA
amtega Axencia para a Modernización Tecnolóxica
igape

acuntia
cellnex driving telecom connectivity
CGES Consello Galego de Enxeñerías
coremain
CRTVG Corporación Radio e Televisión de Galicia
dimension data
emetel
ERICSSON
everis an NTT DATA Company
.gal
gradiant
indra
INEO
Fundación Ingeniero Gerardo García Campos telsis GROUP
ORACLE
orange
paloalto NETWORKS
PSN
R
retegal redes de telecomunicación galegas
satec IT'S easy
SEMI
Smartel
teleco.uvigo.es
telecon
Telefónica
Televes
tesec audiovisuales
ufinet
vodafone
ZENER

Volver ao sumario