MAGAZINE Nº7
#CLOUD

isms forum

ACCELERATING DIGITAL TRANSFORMATION THROUGH THE CLOUD

El Magazine semestral de ISMS Forum - International Information Security Community

ENTREVISTAS

"Una arquitectura de Edge es más compleja en términos de nodos y arquitectura de red, y probablemente más dinámica"

BART PRENEEL

Profesor en la Universidad de Leuven.

FIRMA INVITADA

It's the data, stupid

Cómo migrar hacia un entorno de Data TRUST-formation

BERNARDO GRESRA

Director Académico del Programa Executive en Transformación Digital en IE Business School.

ACTUALIDAD

La nueva certificación de ISMS Forum: Trust-Formation Officer

REDACCIÓN ISMS FORUM

SEPTIEMBRE 2021
www.ismsforum.es

EDITA
ISMS Forum

DIRECTOR GENERAL
Daniel García Sánchez

CONSEJO EDITORIAL, REDACCIÓN, DISEÑO Y MAQUETACIÓN
Raquel García Robles

EQUIPO DE GESTIÓN
Beatriz Lozano Macías
Carmen Granados Ruiz
Cynthia Rica Gómez
Diana Pérez Villa
Leire Ruiz Díaz-Rullo
Raquel García Robles
Virginia Terrasa Bover
Wasim Escribano Lazkani

PÁGINA WEB
www.ismsforum.es

ISMS Forum

Todos los derechos de esta Publicación están reservados a ISMS Forum. Los titulares reconocen el derecho a utilizar la Publicación en el ámbito de la propia actividad profesional con las siguientes condiciones: a) Que se reconozca la propiedad de la Publicación indicando expresamente los titulares del Copyright. b) No se utilice con fines comerciales. c) No se creen obras derivadas por alteración, transformación y/o desarrollo de este Publicación. Los titulares del Copyright no garantizan que la Publicación esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados. El contenido de la Publicación no constituye un asesoramiento de tipo profesional y/o legal. No se garantiza que el contenido de la Publicación sea completo, preciso y/o actualizado. Los contenidos reflejados en el presente documento reflejan el parecer y opiniones de los autores, pero no necesariamente la de las instituciones que representan. Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Publicación son de propiedad exclusiva de los titulares correspondientes.

PRESIDENTE

Gianluca D'Antonio, miembro independiente.

VICEPRESIDENTE

Carlos Alberto Saiz, Ecix Group.

TESORERO

Roberto Baratta, Abanca.

VICESECRETARIO

Francisco Lázaro, RENFE.

SECRETARIO DEL CONSEJO ASESOR

Juan Miguel Velasco.

VOCALES

Xabier Michelena, Accenture Security.
Carles Solé, Banco Santander España.
Gonzalo Asensio, Bankinter.
Virginia Rodríguez, CaixaBank.
Rafael Hernández, CEPSA.
Rubén Frieiro Barros, Deloitte.
Ricardo Sanz, Evolutio.
Edwin Blom, FCC.
Luis Buezo, Hewlett Packard Enterprise.
Susana del Pozo, IBM.
Marcos Gómez, INCIBE.
David Barroso, miembro independiente.
Guillermo Llorente, miembro independiente.
Toni García, miembro independiente.
Jesús Sánchez, Naturgy.
José Ramón Monleón, Orange.
Javier Urtiaga, PwC.
Javier García Quintela, REPSOL.
Agustín Muñoz-Grandes, S21sec.
Iván Sánchez, Sanitas.
Roberto Pérez, SIA.
Miguel Ángel Pérez, Telefónica.
Francisco Javier Sevillano, Vodafone.

JUNTA DIRECTIVA

CONTENIDOS

CARTA DEL PRESIDENTE

Gianluca D'Antonio

La Cloud y la inminente Transformación Digital

ACTUALIDAD ISMS FORUM

Redacción ISMS Forum

ISMS Forum y el Cluster Cyber Madrid establecen un convenio de colaboración

La nueva certificación de ISMS Forum: Trust-Formation Officer

El Nodo Gallego de Ciberseguridad (CIBER.gal) e ISMS Forum forman una alianza con el objetivo de impulsar la ciberseguridad en Galicia

REPORTAJE: Foro Nacional de Ciberseguridad

Redacción ISMS Forum

El Foro Nacional de Ciberseguridad, un espacio de colaboración público-privada dedicado al impulso de la ciberseguridad en España

ISMS FORUM MAG

UN CAFÉ CON LOS EXPERTOS

BART PRENEEL
Profesor en la Universidad de Leuven
"Una arquitectura de Edge es más compleja en términos de nodos y arquitectura de red, y probablemente más dinámica"

FRANCISCO LÁZARO
CISO y DPD de Renfe y Director del IoT Security Centre de ISMS Forum
"Es necesario empoderar a la figura que debe liderar tanto la práctica, como los recursos de la seguridad de la información"

MANUEL VIDAL
Cloud Security Leader, Everis
"Los proveedores de Cloud clase mundial nos enseñan el camino, pero no están dimensionados para recorrerlo con nuestras empresas"

FIRMA INVITADA

BERNARDO CRESPO
Director Académico del Programa Executive en Transformación Digital en IE Business School
It's the data, stupid
Cómo migrar hacia un entorno de Data TRUST-formation

PROYECTOS DE INTERÉS

Redacción ISMS Forum
ISMS Forum y Cloud Security Alliance España publican el XI Estudio del Estado del Arte de Seguridad en la Nube

Consulta la nueva versión de la "Guía para la notificación de brechas de datos personales" de la AEPD

Ya está disponible la "Guía de Gestión de riesgo y evaluación de impacto en tratamientos de datos personales" de la AEPD

CSA-ES, junto con los capítulos de Bolivia, Chile y Perú, traduce al español la Cloud Controls Matrix v4

La Comisión Europea propone la creación de una unidad informática conjunta

GAZINE

CARTA DEL PRESIDENTE

La Cloud y la inminente Transformación Digital

GIANLUCA D'ANTONIO

Presidente de ISMS Forum

ismsforum.es

Estimados profesionales de la Seguridad de la Información y socios de ISMS Forum:

Sin lugar a duda la Nube es hoy un hecho consolidado. Sería difícil imaginar cualquier proceso de transformación sin la Cloud como soporte básico.

La pandemia provocada por la COVID-19 ha supuesto un elemento de aceleración exponencial en este proceso. Si bien la reducción de costes o la flexibilidad siguen siendo impulsores de la adopción de la Nube, las organizaciones también están buscando otras palancas de negocio, desde la agilidad hasta la innovación. Gracias a la Nube las organizaciones ya no tienen que elegir entre calidad, coste y tiempo, pudiendo obtener las tres ventajas a la vez.

La analítica de datos en tiempo real, la escalabilidad y el pago por uso son otros elementos que favorecen este proceso de transformación. La ciberseguridad también se ha visto fuertemente impactada por la adopción de la Cloud. En un primer momento, la ciberseguridad se ocupó de la Cloud como un elemento de riesgo a proteger. En la actualidad, la Cloud está incrementando las capacidades de las tecnologías de la seguridad dotándolas de mayor agilidad, potencia analítica y operación.

Podemos afirmar que la Cloud está llamada a revolucionar la seguridad tradicional tal como la conocemos. De esta dualidad, la Cloud como elemento a proteger y como elemento de protección, los profesionales de la seguridad de la información tendrán que saber extraer el máximo valor si quieren ser embajadores de la transformación digital.

ACTUALIDAD

ISMS FORUM

ACTUALIDAD

ISMS Forum y el Cluster CyberMadrid establecen un convenio de colaboración

Redacción ISMS Forum

El Clúster está promovido por el Ayuntamiento de Madrid, a través del Área de Economía y Hacienda, como parte de sus iniciativas de refuerzo a la competitividad, dentro de su política de promoción de los sectores estratégicos en la Ciudad, y cuenta con la colaboración de la Comunidad de Madrid y el Instituto Nacional de Ciberseguridad.

Desde que el Ayuntamiento de Madrid anunció su creación en 2020, ISMS Forum ha promovido y formado parte de la puesta en marcha del Clúster de Ciberseguridad de Madrid, una asociación sin ánimo de lucro que reúne a empresas, asociaciones e instituciones, tanto públicas como privadas, que desarrollan actividades en el área de Madrid, y que se asocian libremente para impulsar el desarrollo del sector de la ciberseguridad.

La Asociación persigue el objetivo de sensibilizar y formar a empresas y ciudadanos en la importancia crítica de la ciberseguridad, así como reforzar el emprendimiento, incluyendo el desarrollo de nuevas empresas y el crecimiento de las ya existentes. Además de esto, pretende contribuir a generar talento y mejorar la empleabilidad en este ámbito, así como posicionar a Madrid y su región como ciudad impulsora de la ciberseguridad.

Sus actividades están enfocadas al fomento de la formación y capacitación para la mejor cualificación de profesionales, la promoción y desarrollo de proyectos de I+D+i en el sector, y la organización de cursos de formación en materia de ciberseguridad, entre otras. Como primera iniciativa, junto a ISMS Forum, el Clúster ha presentado el proyecto Pyme 3DSecure a la consulta pública convocada por el Ministerio de Asuntos Económicos y Transformación Digital, cuyo objetivo es el de mejorar la postura de Ciberseguridad de las pymes.

La nueva certificación de ISMS Forum: Trust-Formation Officer

Redacción ISMS Forum

ISMS Forum, a través de la CISO Academy, una nueva iniciativa centrada en el empoderamiento de la figura profesional del Director de Seguridad de la Información, ha creado la certificación "Trust-Formation Officer Certification", orientada a servir de ayuda a los CISOs a la hora de comprender mejor las prioridades de negocio, las nuevas tecnologías producto de la Transformación Digital y el contexto de compliance legal.

Con el objetivo de crear una verdadera comunidad en torno al rol profesional del Chief Information Security Officer (CISO), ISMS Forum ha puesto en marcha la CISO Academy, una iniciativa de valor centrada en el empoderamiento de la figura profesional del Director de Seguridad de la Información que trata de establecer un escenario formativo práctico que permita su formación y actualización continua, mejorando asimismo su posición e interlocución interna con el C-Level de la organización.

De esta iniciativa nace la certificación "Trust-Formation Officer Certification", la primera certificación española dirigida a la figura del CISO. Se trata de un programa formativo que consta de cinco dominios basados en las principales líneas estratégicas de acción que impone el proceso de Transformación Digital que vivimos: Ciberseguridad en la Cloud, Continuidad del negocio, Transformación Digital, GRC y El CISO en el Board.

El programa formativo, cuya duración es de dos años, ayudará a los Directivos de Seguridad de la Información a comprender mejor las prioridades de negocio, las nuevas tecnologías producto de la Transformación Digital y el contexto de compliance legal.

La obtención de la certificación acredita el reconocimiento del ejercicio de la profesión a través de los cinco módulos independientes y cuya superación comporta un reconocimiento por cada uno de los bloques formativos que la componen.

El Nodo Gallego de Ciberseguridad (CIBER.gal) e ISMS Forum forman una alianza con el objetivo de impulsar la ciberseguridad en Galicia

Redacción ISMS Forum

El nodo gallego de ciberseguridad (CIBER.gal), es una estructura de cooperación en Ciberseguridad para el desarrollo de actividades que sensibilicen y formen a ciudadanos, empresas y administraciones públicas de la Comunidad Autónoma de Galicia en ciberseguridad. En su compromiso con la Seguridad de la Información, ISMS Forum y su capítulo gallego, han firmado un acuerdo de colaboración para ayudar a promover esta labor de sensibilización, concienciación, capacitación y formación en ciberseguridad.

CIBER.gal desarrolla sus funciones a través de una Comisión de Seguimiento formada por los firmantes del convenio de colaboración (Xunta de Galicia, Diputaciones de Galicia, FEGAMP, INCIBE y CCN) y contando con tres grupos de trabajo: Ciudadanía, Administración Pública y Empresa. Por su parte, ISMS Forum se compromete a colaborar con el cumplimiento de los objetivos del nodo, entre los que destacan:

- Impulsar acciones dirigidas a la sensibilización, concienciación, capacitación y formación en ciberseguridad, tales como eventos, seminarios o talleres, dirigidos a la ciudadanía, empresas y Administraciones Públicas en la Comunidad Autónoma Gallega.

- Colaborar para dar respuesta conjunta a los retos tecnológicos relacionados con la seguridad de la información que sean expuestos en colectivos o entidades a las que prestan servicio.

- Promover la generación de conocimiento, creación y retención de talento especializado en materia de Seguridad de la Información, y el impulso de iniciativas para la transferencia e intercambio de conocimiento y experiencias o proyectos en ciberseguridad.

- Colaborar técnica u operativamente en la gestión y respuesta a incidentes que pudieran afectar la cada una de las partes o a los colectivos a los que se presta servicio.

- Participar en acciones de fomento de la I+D+i y del emprendimiento y en el impulso a la industria de la ciberseguridad, incluyendo iniciativas de colaboración público-privada.

Para todo ello, se crearán grupos de trabajo que se encargarán de promover y dinamizar la cooperación entre instituciones, empresas y sociedad para hacer frente al reto de vivir en un entorno seguro.

REPORTAJE

Foro Nacional de Ciberseguridad

REPORTAJE

El Foro Nacional de Ciberseguridad, un espacio de colaboración público-privada dedicado al impulso de la ciberseguridad en España

Redacción ISMS Forum

En julio de 2020 tuvo lugar una reunión virtual para la constitución del Foro Nacional de Ciberseguridad. Esta estuvo presidida por el director del Gabinete de la Presidencia del Gobierno, Iván Redondo, acompañado por Miguel Ángel Ballesteros, director del Departamento de Seguridad Nacional y presidente del Foro; las dos vicepresidencias del Foro: la directora general del INCIBE y el subdirector del CCN; así como los vocales designados por las organizaciones que los constituyen.

Las líneas de trabajo establecidas Están centradas en generar cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y una oportunidad para la formación y el talento en ciberseguridad; todas ellas alineadas con las medidas recogidas en la Estrategia Nacional de Ciberseguridad 2019.

Varios principios serán claves de acción de este Foro: la unidad de acción, la transparencia y accesibilidad, la adaptabilidad y flexibilidad, la participación abierta y el compromiso, así como la responsabilidad compartida y la reciprocidad. Unos principios que se articularán en un entorno de colaboración público-privada, de la que ISMS Forum ya forma parte, donde compartir y generar conocimiento sobre las oportunidades y los desafíos para la seguridad en el ciberespacio bajo el paraguas del Consejo Nacional de Ciberseguridad.

¿Cómo está compuesto?

- Presidencia: La presidencia será ejercida por el vicepresidente del Consejo Nacional de Ciberseguridad y director del Departamento de Seguridad Nacional. Cuando se considere oportuno y, al menos, una vez al año, el presidente del Consejo Nacional de Ciberseguridad presidirá la reunión del Foro.

- Vicepresidencias: Existirán dos Vicepresidencias:

  - La Vicepresidencia Primera será ejercida por el director del Instituto Nacional de Ciberseguridad de España.

  - La Vicepresidencia Segunda será ejercida por el subdirector del Centro Criptológico Nacional.

- Secretaría: Las funciones de Secretaría del Foro serán desempeñadas por el Departamento de Seguridad Nacional. Cada Grupo de Trabajo designará un presidente y una Secretaría. El secretario será designado por el presidente del Foro, entre el personal perteneciente al Departamento de Seguridad Nacional, asumiendo además de las funciones propias de secretario, las de apoyo al presidente del Foro.

- Vocalías: El Foro estará compuesto por vocales representantes de diferentes organizaciones.

- Vocalías Permanentes: compuestas por un representante de cada uno de los miembros de la Comisión Permanente de Ciberseguridad.

La Presidencia del Foro propondrá al Consejo Nacional de Ciberseguridad el nombramiento como Vocales del Foro, a actores que representen intereses económicos, industriales, académicos o sociales colectivos y organizados, así como a representantes de la administración.

También podrá formar parte del Foro un representante del sector que se determine, cuya presencia sea así acordada por el presidente/a del Foro, en función de los asuntos a tratar.

Asimismo, podrán ser convocados en función de la naturaleza de los asuntos que se traten en el orden del día otros representantes de la red de expertos nacionales, de las Comunidades Autónomas, de las Ciudades con Estatuto de Autonomía y de las entidades locales. Igualmente podrán ser convocados aquellas personas en su condición de expertos cuya contribución se considere relevante.

El Consejo Nacional de Ciberseguridad, una vez examinada la propuesta de nombramiento para ocupar una Vocalía del Foro en los términos expuestos, aprobará o denegará la misma.

Este Foro se reunirá a iniciativa del presidente como mínimo dos veces al año o cuantas veces lo considere necesario en función de las circunstancias que afecten a su ámbito de actuación.

El orden del día será acordado su presidente, una vez analizadas las propuestas de los miembros del Foro.

22 de julio de 2020, reunión para la constitución del Foro Nacional de Ciberseguridad. En la imagen, los representantes del Gobierno, DSN, INCIBE y CCN.

Los objetivos del Foro

El Foro Nacional de Ciberseguridad se encargará de proponer iniciativas al Consejo Nacional de Ciberseguridad, desde la perspectiva del sector privado, para la potenciación y creación de sinergias público-privadas en materia de ciberseguridad o ciberdefensa. Asimismo, analizará y estudiará propuestas, propias o encomendadas, que permitan apoyar la toma de decisiones del Consejo Nacional de Ciberseguridad, contribuyendo a la valoración y análisis de los riesgos y amenazas respecto a la ciberseguridad, junto a la propuesta de acciones de mitigación y respuesta.

Otra de sus funciones será la de apoyar la realización y evaluación de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y la ciberdefensa y contribuir a la identificación de las necesidades de la industria y de los centros de investigación, en lo que se refiere a ciberseguridad.

Por otro lado, colaborará en la realización de catálogos de recursos que identifiquen los medios y capacidades del sector privado y la sociedad civil, con la finalidad de determinar las medidas de respuesta más eficaces en consonancia con los medios disponibles y las misiones a realizar.

El Foro canalizará y formulará propuestas sobre el marco regulatorio y normativo con incidencia sobre la ciberseguridad, considerando asimismo otras disciplinas relacionadas que debieran armonizarse entre sí, e impulsará la realización proactiva de

estudios e informes sobre tecnologías nuevas y emergentes y analizar su impacto en la ciberseguridad nacional, a la vez que, de forma reactiva, realizarlo a petición del Consejo Nacional de Ciberseguridad.

El objetivo final es idear iniciativas tendentes a promover la cultura Nacional de Ciberseguridad, apoyando la proyección y participación de España a nivel internacional y europeo en materia de ciberseguridad y ciberdefensa.

Como comentó Mar López, antigua Jefa de la Unidad de Ciberseguridad y lucha contra la desinformación en el DSN y promotora del Foro Nacional de Ciberseguridad, para una entrevista con ISMS Forum: "El objetivo del Foro Nacional de Ciberseguridad es incrementar la colaboración de la sociedad civil y el sector privado en materia de ciberseguridad, tan necesaria en estos momentos en los que nos encontramos".

Para ello, a principios de junio, el Foro Nacional de Ciberseguridad definió las acciones que se iban a desarrollar en los tres grupos de trabajo creados para fomentar la cultura de ciberseguridad, el impulso a la industria y a la I+D+i, y la formación, capacitación y talento.

El grupo de trabajo centrado en la cultura de ciberseguridad, coordinado por ISMS Forum junto a la Fundación Borredá, se focalizará en proponer actuaciones para incrementar las campañas de concienciación, potenciando la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional, e impulsando iniciativas y planes de alfabetización digital en ciberseguridad. También tratará de promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial reconociendo la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad corporativa.

Es por este motivo, que abordarán la concienciación y formación en ciberseguridad desde los directivos de organizaciones, tratando de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar, hasta los centros de enseñanza, para que puedan adaptarse a todos los niveles de formación y especialidades, colaborando y participando en diferentes medios de comunicación con el objetivo de lograr un mayor alcance en las campañas dirigidas a ciudadanos y menores de edad.

Uno de los proyectos que llevará a cabo este grupo de trabajo, será el Libro Blanco de la cultura de la ciberseguridad.

Por su parte, el grupo de trabajo encargado de proponer actuaciones para impulsar la industria y la I+D+i, deberá estimular el incremento de la oferta y demanda de productos y servicios de ciberseguridad de la industria española, así como su internacionalización, e incrementar el peso de la industria española de ciberseguridad en el mercado europeo y global. Para ello, desarrollarán el Libro Blanco sobre el sector de la ciberprotección en España. Lo que se pretende es generar las condiciones para un ecosistema de emprendimiento en ciberseguridad, de manera que las pymes, micropymes y autónomos, puedan acceder y adoptar medidas en ciberseguridad.

Por último, el grupo de trabajo encargado de la formación, capacitación y talento en ciberseguridad, en el que ISMS Forum ha tomado gran parte activa, desarrollará marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral identificando las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas, impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional. Una de las iniciativas en las que está inmerso este grupo de trabajo es la creación de un esquema de certificación nacional centrado en el Responsable de Ciberseguridad.

El objetivo del Foro Nacional de Ciberseguridad es incrementar la colaboración de la sociedad civil y el sector privado en materia de ciberseguridad, tan necesaria en estos momentos en los que nos encontramos.

UN CAFÉ CON

LOS EXPERTOS

ENTREVISTAS

"El movimiento hacia el Edge puede combinarse con fuertes medidas de seguridad y aislamiento, esto puede dar lugar a una arquitectura de privacidad desde el diseño"

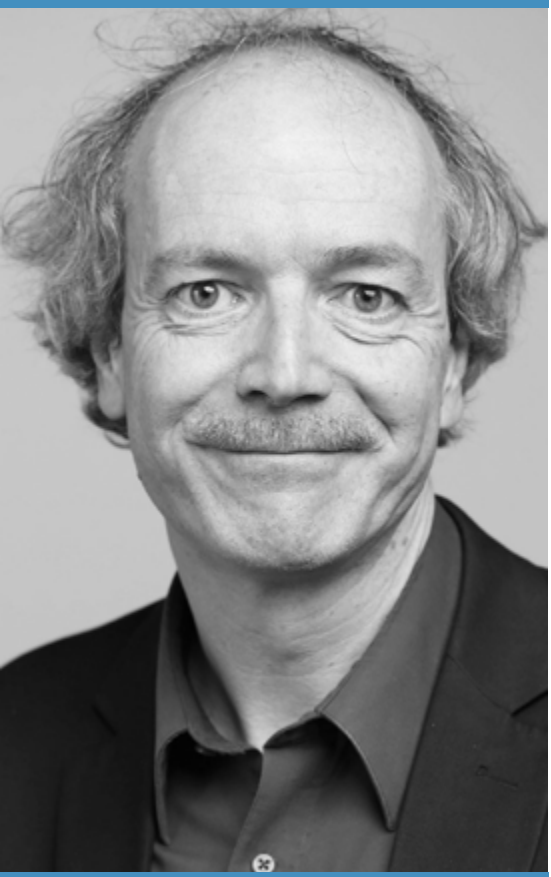
Bart Preneel dirige el grupo de investigación COSIC de la Universidad KU Leuven, que cuenta con 100 miembros. Sus principales intereses de investigación son la criptografía, la seguridad de la información y la privacidad. Es autor de más de 400 publicaciones científicas e inventor de cinco patentes. Ha sido presidente de la IACR (International Association for Cryptologic Research) y es miembro del grupo asesor de ENISA, y de la Academia Europea y del Centro de Conocimiento de la Autoridad Belga de Privacidad. También ha sido ponente invitado en más de 130 conferencias en 50 países y ha recibido el premio RSA a la excelencia en el campo de las matemáticas. Asimismo, es consultor habitual de la industria y la administración sobre tecnologías de seguridad y privacidad, y cofundador de la startup nextAuth, formando parte del consejo de administración y del consejo asesor de varias empresas.

La madurez ha llegado a la Nube. ¿Estamos ante la próxima revolución de la ciberseguridad en el Edge?

El Edge está surgiendo como un nuevo paradigma informático, impulsado en gran medida por la necesidad de reducir la latencia y el ancho de banda para permitir la toma de decisiones locales. Los nodos locales del Edge son esenciales para permitir el desarrollo de la nueva robótica, los vehículos autónomos y la realidad virtual y ampliada. Por desgracia, la experiencia nos ha enseñado que la seguridad y la privacidad tienden a quedar en segundo plano cuando se despliegan nuevas tecnologías. Por lo tanto, cabe esperar que se identifiquen nuevas vulnerabilidades y modos de fallo y que posteriormente se den respuestas. Uno esperaría que las lecciones aprendidas del pasado y la evolución del contexto legal (incluyendo el RGPD y la Directiva NIS) estimularan una actitud más proactiva, pero quizá eso es ser demasiado optimista.

¿Qué ventajas generará el Edge en el ámbito de la ciberseguridad?

El tratamiento de los datos a nivel local presenta claras ventajas en materia de seguridad y privacidad. Si el movimiento hacia el Edge puede combinarse con fuertes medidas de seguridad y aislamiento, esto puede dar lugar a una arquitectura de privacidad desde el diseño, tal y como exige el RGPD. Esto implica que la



BART PRENEEL

Profesor de la Universidad de Leuven.

mayoría de los datos permanecen locales bajo el control de los usuarios y solo un mínimo de datos se recogen de forma centralizada. Esto supone una gran mejora con respecto a las soluciones en las que todos los datos acaban en un único lugar. Por ejemplo, las técnicas de aprendizaje federado permiten entrenar a los sistemas de IA y tomar decisiones localmente, mientras se intercambia solo información de alto nivel con los servidores centrales. Como ventaja adicional, si las cosas van mal, se reduce el impacto de las violaciones de la seguridad y la privacidad.

A nivel normativo, ¿será un mejor escenario para el cumplimiento?

Como he mencionado anteriormente, a un alto nivel, este enfoque descentralizado está en principio mejor alineado con los principios de "minimización de datos" y "privacidad por diseño", tal como exige el RGPD. Una arquitectura de Edge es más compleja en términos de nodos y arquitectura de red, y probablemente más dinámica. Incluso con un correcto aislamiento y una fuerte seguridad, asegurar una red tan compleja es más difícil. Esto también presenta mayores desafíos en términos de auditoría y certificación de sistemas.

¿Cuáles son los desafíos para una implementación exitosa?

Asegurar un sistema complejo siempre presenta un amplio abanico de retos en cuanto a varios aspectos:

1) la gestión de la configuración 2) la seguridad de los nodos (por ejemplo, la autenticación de los nodos, la protección de los datos en los nodos, el procesamiento seguro y la gestión del ciclo de vida global de forma segura) y 3) la seguridad de la red (comunicaciones seguras, enrutamiento seguro, protección contra ataques DDOS). Aparte de la mayor complejidad, el aumento de la vulnerabilidad de los nodos de Edge a los ataques físicos presenta retos adicionales: esto puede tratarse mediante una combinación de técnicas de protección física (resistencia a la manipulación, puesta a cero) y técnicas de supervisión.

¿Se ampliará la brecha digital entre las PYMES y las grandes empresas?

Aunque las PYMES dependen cada vez más de las tecnologías digitales, cuentan con presupuestos limitados en materia de TI y seguridad informática, así como con escasos conocimientos técnicos para hacer frente a un número creciente de complejos retos en materia de seguridad y privacidad. Si no se interviene, esto conducirá a una brecha cada vez mayor con las organizaciones más grandes. Aunque no existe una bala de plata, es necesario un enfoque estratégico que consista en campañas de concienciación, el desarrollo de soluciones fáciles de usar que sean "seguras y privadas por diseño" y que requieran una configuración y gestión mínimas, y la externalización de parte de la gestión de estas solu-

Una arquitectura de Edge es más compleja en términos de nodos y arquitectura de red, y probablemente más dinámica. Incluso con un correcto aislamiento y una fuerte seguridad, asegurar una red tan compleja es más difícil.

Un reto central para la criptografía sigue siendo la gestión eficaz de las claves: esto incluye todos los aspectos, desde la generación hasta el almacenamiento, la distribución, el archivo y la destrucción.

ciones a partes especializadas. Aunque hay algunos avances en el mercado en esta dirección, es necesario el apoyo de los gobiernos, así como el de los grandes actores con más experiencia, que dependen en gran medida de estas PYMES.

¿Qué riesgos conlleva la implantación de este nuevo modelo?

Llevamos más de dos décadas de experiencia en la protección de redes y dispositivos a gran escala. Seguimos cometiendo muchos errores, pero estamos aprendiendo. Sin embargo, como ocurre con cualquier nuevo modelo, el modelo de Edge hará que se identifiquen y exploten nuevas vulnerabilidades. Esto se ve agravado por la mayor complejidad del sistema global y por la falta de seguridad física de los nodos de Edge. El principal riesgo es que no aprendamos de nuestros errores anteriores y empecemos a desplegarlo antes de entender completamente cómo asegurarlo.

¿Qué hay del control sobre los datos, los procesos y la tecnología?

El Edge permite el control local de los datos, los procesos y la tecnología. Sin embargo, debido al aumento del tamaño y la complejidad del sistema global del Edge y la Nube, parece probable que los controles sean automatizados. Esto implica que los datos, el procesamiento y los dispositivos son locales, pero las decisiones clave de gobernanza sobre se-

guridad y privacidad se tomarán de forma centralizada. En consecuencia, sigue existiendo un riesgo de abuso de la privacidad (la información seleccionada, como el resultado del complejo procesamiento de los Edge, se está centralizando); también significa que si el sistema de control central se ve comprometido, el sistema global se ve afectado. En este sentido, no espero que los sistemas de Nube o de Edge y Nube sean muy diferentes en términos de controles.

Desde el punto de vista criptográfico, ¿cuáles son los retos venideros?

El coste de la seguridad de las comunicaciones y los datos almacenados con criptografía ha descendido drásticamente en las últimas décadas. Sin embargo, sigue siendo necesario mejorar el rendimiento y, en particular, reducir la latencia. Un reto central para la criptografía sigue siendo la gestión eficaz de las claves: esto incluye todos los aspectos, desde la generación hasta el almacenamiento, la distribución, el archivo y la destrucción. A largo plazo, uno de los principales retos es pasar a la criptografía poscuántica; esto afecta sobre todo al establecimiento de claves públicas y a las firmas digitales. Cabe esperar que el proceso de estandarización del NIST en este ámbito finalice a principios de 2023; posteriormente, será necesario un esfuerzo de despliegue sostenido de 5 a 7 años. Un último reto será desplegar la criptografía para proteger los datos mientras se procesan. Técnicas como la computación multipartita y el cifrado totalmente homomórfico requieren hoy en día una cuidadosa puesta a punto de las aplicaciones y solo son adecuadas para ciertos nichos; serán viables para un número creciente de aplicaciones a medida que su coste pueda reducirse aún más durante la próxima década.

En tu opinión, ¿cómo debería ser una arquitectura de seguridad en la Nube de próxima generación?

Las futuras arquitecturas de seguridad tendrán que encontrar el equilibrio adecuado entre la centralización y la descentralización: aunque los sistemas centralizados presentan claras ventajas en términos de control y visibilidad, presentan puntos únicos de fallo; además, los sistemas centralizados conllevan el riesgo de abuso de datos sensibles y de grandes violaciones de datos. La descentralización es muy prometedora, pero requiere un enfoque de diseño cuidadoso. Las arquitecturas del futuro utilizarán la criptografía para proteger los datos mientras están almacenados, en tránsito o durante el procesamiento; este enfoque de seguridad "todo incluido" tiene que conciliarse con la transparencia y la responsabilidad, en términos del procesamiento que se está realizando. Además, hay que hacer esfuerzos considerables para que todos los componentes sean más robustos y para construir un entorno de confianza cero en el que cada componente esté totalmente autentificado frente a todos los demás.

"Es necesario empoderar a la figura que debe liderar tanto la práctica, como los recursos de la seguridad de la información"

Francisco Lázaro

CISO y DPD de Renfe y Director del IoT Security Centre de ISMS Forum.

Francisco Lázaro es gerente de Ciberseguridad y Privacidad (CISO y DPD) de Renfe y Director del IoT Security Centre de ISMS Forum. También es profesor Asociado en la ETSI de telecomunicaciones de la UPM y profesor en diversos másteres Universitarios de Ciberseguridad. Asimismo, es Delegado de Seguridad de infraestructura Crítica, Presidente del Grupo de Calidad y Seguridad de AUTELSI, miembro de diversos grupos de Normalización UNE e ISO y miembro de la Junta Directiva de la Asociación Española de Ejecutivos y Financieros, así como Vocal en el Foro Nacional de Ciberseguridad. También está en posesión de la habilitación del Ministerio del Interior como Director de Seguridad.

¿De dónde surge la necesidad de actualizar el Esquema Nacional de Ciberseguridad?

Tanto en la redacción del anterior Real Decreto Ley del Esquema Nacional de Seguridad como en el nuevo Proyecto de Real Decreto (PRD), en su artículo 39 establece que el Esquema Nacional de Seguridad (ENS) se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en

paralelo al avance de los servicios prestados por las entidades del sector público, a la evolución tecnológica y a la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría.

Por tanto, el grupo de responsables de normativa de las entidades públicas que proponen la regulación del ENS a sus respectivos Ministerios han convenido que, ha llegado ese momento y para ello deben armonizarla con otras legislaciones y evolucionarla conforme a referido en el artículo 39.

Armonizarla, con otras regulaciones con las que tengan una "superficie de contacto" en el alcance, evitando no solo no entrar en colisión con ellas (por ejemplo con preceptos contrarios) sino buscando complementarse, incluyendo aspectos de seguridad de la información, que no estén presentes en las otras leyes pero que estén dentro del alcance que tengan en común o bien, mediante el desarrollo de algún punto en el que otra u otras legislaciones se refirieran al ENS en su articulado; como ocurre por ejemplo, tanto en la trasposición de la NIS, como en la LOPDyGDD.

En mi opinión, el resultado armonizador plasmado en el PRD no va más allá de recoger aquellos aspectos que le afectan al CCN, tales como la responsabilidad del CCN-CERT en la gestión de los incidentes. Al PRD se le ven las costuras en otros aspectos armonizadores que no trata. Por ejemplo, es clamoroso el silencio, cuando no sangrante, la nula armonización con el artículo 7 del RD 43/2021 en relación con las funciones, posición e independencia del responsable de seguridad.

Este "olvido", probablemente es debido, a que en el grupo de redacción han primado otros intereses: no alterar la plantilla de las pequeñas entidades locales, no evidenciar que hay un coste por el ejercicio del rol y de su responsabilidad y finalmente, por intentar (en mi opinión erróneamente) buscar un papel homogéneo para el Comité de Seguridad, en un mundo tan heterogéneo de necesidades y recursos, como el que encontramos en el sector público.

El ENS debe evolucionar para cubrir el mayor alcance que la Ley 40/2015 le asigna, tanto en el alcance objetivo (a qué aplica) como subjetivo (a quién aplica). Originariamente el ENS alcanzaba solamente a las Administraciones Públicas y ciudadanos, mientras que por la 40/2015 ahora aplica a todo el Sector Público. Lo mismo pasa con los sistemas, que originalmente eran los que permitían relacionar a los administrados con la administración y ahora es cualquier sistema involucrado en el ejercicio de sus competencias y potestades administrativas; es decir para cualquier servicio.

También debe evolucionar en lo relativo a los controles, con la retirada de unos pocos de estos que ya no son necesarios y la inclusión de un par de ellos, como los referidos a la Nube, que no podían obviarse.

¿Qué evolución, respecto al anterior ENS, podemos encontrar en las medidas técnicas y organizativas para prevenir y reducir al mínimo los efectos de los ciberincidentes?

El PRD apoyado en los principios básicos y requerimientos mínimos busca que las

entidades del sector público mejoren su seguridad y por tanto la gestión de los incidentes, con una más ajustada elección de controles y eso lo articula en esta versión con los llamados "refuerzos" y perfiles y con las acreditaciones. Estos "recursos" técnicos deben dar la capacidad adecuada a una gestión de riesgos más ajustada. Para tal fin y para graduar una mayor exigencia, el PRD emplea lo que denomina los refuerzos de seguridad (R), los cuales se suman a los requisitos base de la medida pero que no siempre son incrementales entre sí. Se pueden combinar o elegir refuerzos diferentes. Esta mayor granularidad junto con los perfiles, permiten ajustar más los controles.

Igualmente, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con el real decreto.

En cuanto a las obligaciones de las organizaciones del sector privado que presten servicios a las entidades públicas, ¿qué cambios se han producido?

Las empresas del sector privado que prestan servicios a entidades públicas también deben cumplir los requerimientos del ENS según el tipo de servicio e información que tratan y esa obligación no se limita solo a las empresas tecnológicas. Esta obligación estaba ya presente en el actual conjunto de documentos que desarrollan el ENS, si bien no se recogía explícitamente en el texto de la Ley, como si lo hace ahora el PRD.

Curiosamente, la obligación de cumplir con el ENS por parte de un proveedor no será la primera vez que aparece a nivel de ley, pues ya en la disposición adicional primera de la LOPDyGDD, *Medidas de seguridad en el ámbito del sector público* se dice que en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

La obligación se establece en el PRD a través de tres cuestiones esenciales:

- La obligación de reportar
- La obligación de cumplir
- La obligación de hacer cumplir.

Estas obligaciones a los proveedores no solo aplican a empresas tecnológicas y de servicios TIC; por ejemplo, a empresas de desarrollo de software, servicios Cloud o mantenimiento de sistemas, sino que los proveedores del sector público deberán cumplir el ENS ya sea por tratar datos de carácter personal o en general, por el mero hecho de procesar información, de cualquier tipo que sea responsabilidad de la administración, en servicios tales como nóminas, contabilidad, publicidad, seguros, servicios médicos, formación, etc. Siempre claro está, para el alcance del servicio del que formen parte como principal o como cadena de suministro de este.

¿Qué funciones establece el Real De-

creto para el Responsable de Seguridad de la Información frente a la figura del Comité de Seguridad?

El PRD no da relevancia al Responsable de Seguridad de la Información, no está al nivel de concreción y de acierto del RD 43/2021 del 26 de enero, en su artículo 7, donde se concretan las funciones principales del Responsable de Seguridad de la Información, de la necesidad de dotarle de medios, de su posición en la organización y de la independencia de la dirección de sistemas.

Al Responsable de Seguridad de la Información frente al Comité se le otorga un papel secundario. Aunque para hacer la comparación deberemos salir del PRD, pues en su texto tan solo menciona al Comité en dos párrafos; como comité de gestión y de coordinación de la Seguridad. Para ir al detalle debemos consultar las guías STIC, en concreto la *STIC-801 Responsabilidades y funciones* en la que al Comité se le asigna el gobierno de la Seguridad, responsabilizándole de alinear las actividades de la organización en materia de seguridad de la información. Al Responsable de Seguridad, el ENS le da un papel tan poco relevante que, por ejemplo, no lo menciona entre las fuentes de asesoramiento de los temas sobre los que tenga el Comité que decidir o emitir una opinión. La guía dice cosas tan curiosas como que en el punto que habla del CSO y del CISO, del primero se dice que se le requiere la visión del Negocio; como si el CISO no la debiese tener.

La fuente del error de nuevo reside en que al buscar el CCN un modelo común de Or-

El PRD no da relevancia al Responsable de Seguridad de la Información, no está al nivel de concreción y de acierto del RD 43/2021 del 26 de enero, en su artículo 7, donde se concretan las funciones principales del Responsable de Seguridad de la Información.

ganización para todas las entidades, lo ha focalizado en las entidades locales, poniendo toda la fe en que el regidor de la entidad, presidiendo el comité dirija la función.

¿Cuál es el punto de atención sobre los operadores de servicios esenciales?

Mucho y poco, aunque suene a contradictorio. Mucho porque en el artículo 6 del RD 43/2021 en las obligaciones del operador se establece que las medidas que se aplicarán en los servicios esenciales tomarán como referencia las recogidas en el anexo II del Esquema Nacional de Seguridad y en consecuencia todos los controles de este PRD son referencia para los operadores, y poco, pues en el propio PRD casi no hay referencias a los operadores esenciales. Hay una referencia a lo que acabo de decir del artículo 6 del RD 43/2021 y otra a la gestión de incidentes que deberán seguir la instrucción técnica del CCN al respecto, así como del anexo del RD 43/2021 de notificación y de uso de la plataforma (hasta ahora no implementada) de notificación unificada que debería ser provista por el CCN.

Es justo resaltar la contradicción resultado de la falta de armonización entre el ENS y los servicios esenciales que se deriva de la disparidad de funciones y garantías del Responsable de Seguridad de la Información a las que se obligan a los operadores esenciales, frente a la parquedad de funciones y nulas garantías para el desarrollo de su función del Responsable de Seguridad a las que se obligan a las entidades del sector público.

¿Cómo ha integrado los cambios regulatorios recientes en el contexto europeo?

Todas las regulaciones que están apareciendo a nivel Europeo nos hablan, por una parte, de que los sujetos obligados deben tener como pilar principal la realización de análisis de riesgos, que deben llevar a cabo la gestión y notificación de incidentes y, por otra parte, de las obligaciones de los estados miembros, tales como designar al menos una autoridad de control, disponer de al menos un CERT, así como una coordinación nacional y de cara al resto de la Unión. En ese contexto, el PRD trata para su alcance objetivo y subjetivo, todas esas cuestiones e incluso se adelanta en el tiempo a las obligaciones de la cadena de suministro que aparecen en el borrador temprano de la NIS2.

En tu opinión, ¿en qué aspectos habría que seguir trabajando?

Habría que seguir trabajando en la armonización con el RD 43/2021 en lo referente al Responsable de Seguridad de la Información. Lo que debería traducirse en un reconocimiento de sus funciones y en las garantías para el desarrollo de su función (medios, posición en la organización e independencia de sistemas).

Esta opinión, no es consecuencia de un pensamiento de defensa gremial, sino del convencimiento de que es necesario empoderar a la figura que debe liderar tanto la práctica, como los recursos de la seguridad de la información. Liderazgo, que el proyecto si reconoce en la figura del punto de contacto del proveedor y que sin embargo no lo hace con el responsable de la información de la entidad.

"Los proveedores de Cloud clase mundial nos enseñan el camino, pero no están dimensionados para recorrerlo con nuestras empresas"

Manuel Vidal es Licenciado en Informática por la Universidad Politécnica de Madrid. Tiene un EXMBA por el Instituto de Empresa, un PDG por IESE y un Master en Ciberseguridad por la UCAM.

Cuenta con más de 30 años de experiencia en el sector de las tecnologías de la información, en el que ha desempeñado funciones de desarrollo de software, arquitectura de soluciones, implementación de ERPs, dirección de proyectos y servicios gestionados y distintas posiciones de Dirección en E&Y, Indra, Sun Microsystems, Oracle, Deloitte y Everis-NTT Data. Los últimos 5 años ha estado enfocado casi exclusivamente en Cloud, identidad y ciberseguridad.

MANUEL VIDAL

Cloud Security Leader, Everis.

Desde una perspectiva de seguridad, ¿cómo la Cloud puede actuar como catalizador de la Transformación Digital?

Para aportar cierto rigor habría que diferenciar entre IaaS, PaaS y SaaS.

Un proveedor de clase mundial de SaaS va a disponer de mejores medidas de seguridad que el 99% de sus clientes finales, por lo que SaaS es un facilitador, ya que minimiza el nivel de riesgo de la mayoría de sus clientes.

Con IaaS y PaaS, ocurre algo similar, pero

no exactamente igual, un CSP de clase mundial aporta más recursos de seguridad de los que pueden implementar el 99% de sus clientes finales; pero el cliente tendrá que pagar la mayoría de dichos servicios y tendrá que configurarlos adecuadamente. Hoy en día, la mayoría de esas organizaciones no disponen del conocimiento y experiencia suficientes para realizar esa configuración.

En entornos híbridos la situación se complica. Pasamos de un entorno propio a un entorno en el que servicios propios se integran con los de un tercero que no conocemos perfectamente.

En entornos multiCloud la situación se complica aún más y habrá que recurrir a grandes integradores y proveedores de servicios de seguridad en SaaS que sean asépticos.

Resumiendo, los proveedores de Cloud clase mundial nos enseñan el camino, pero no están dimensionados para recorrerlo con nuestras empresas.

¿Cuál es la evolución en los servicios gestionados en la Cloud tras la situación de pandemia?

Los servicios gestionados de colaboración en la Cloud han permitido operar a muchas organizaciones durante la pandemia, sin ellos muchas se habrían paralizado.

Adicionalmente, la mayoría de los servicios gestionados en la Cloud han disfrutado de grandes crecimientos en sus tasas de adopción y consumo. Se ha demostrado que es mucho más ágil contratar un servicio de Consumer SaaS o de Business SaaS que construirlo internamente. Los departamentos de seguridad han tenido que tomar muchas decisiones muy rápidamente para habilitar su uso.

Los servicios IaaS y PaaS también han crecido como consecuencia de la pandemia, pero siguen necesitando una profunda implicación de los departamentos de TI y por supuesto de seguridad.

Lo normal es que según se vaya normalizando la situación tras la pandemia, se vayan homogeneizando los tratamientos de los distintos servicios gestionados que han sido contratados desde el comienzo de la misma. La tasa de consumo de algunos de ellos decrecerá con la vuelta a los centros de trabajo.

¿Cómo observa la evolución tanto del número de incidentes como la criticidad de los mismos en el ámbito Cloud?

El crecimiento del número de incidentes en la Cloud es proporcional al incremento de la tasa de adopción y uso.

La mayor criticidad de los mismos se debe a que las organizaciones están adoptando servicios cada vez más críticos y están migrando servicios cada vez más críticos, cualquier incidente pasa a tener mayor relevancia sobre la actividad de la organización.

A estos factores se añade la adopción prematura de algunos servicios ante la posibilidad de tener que paralizar la organización, alguien tomó la decisión de asumir los riesgos.

En mi opinión, se debe invertir mucho más tiempo en todo lo relacionado con identidad, autenticación y autorización por una parte; y por otra, y no menos importante, en la configuración de los servicios contratados.

¿A qué riesgos se exponen las empresas que contratan este servicio? ¿Y en sus relaciones con terceros?

Hay un subconjunto de riesgos adicionales a los ya conocidos en el mundo tradicional. En mi opinión, el mayor riesgo es la escasez de conocimiento de la seguridad de los entornos Cloud, lo que provoca numerosos problemas de configuración de los servicios. Es un riesgo que se va minimizando lentamente, porque hay muchos profesionales que van adquiriendo el conocimiento y la experiencia.

Se habla también del riesgo de las tecnologías compartidas en la Cloud, y aunque es real, no veo fácil materializar ese riesgo en un ataque dirigido a una organización.

El riesgo de los equipos humanos de los CSPs ya existe hoy en día con los equipos internos, y es incluso inferior al de estos.

Los riesgos en cuanto a los terceros son similares, si perjudicamos a un tercero, este no va a discriminar si tenemos nuestros servicios "on-prem" o en un CSP de clase mundial. Si tenemos contratados servicios en un CSP de segundo nivel, tendremos que dar más explicaciones.

Ante un incidente en la cadena de suministro, ¿cuál es el protocolo de role back que plantea la Cloud?

Los grandes proveedores de Cloud tienen mecanismos automatizados de actualización de sus activos software en la Cloud. No debemos tener ninguna duda que se producirá algún gran incidente en la cadena de suministro que afectará a alguno de los proveedores hiperescalares. Todos esperamos que sus equipos de respuesta ante incidentes, sus mecanismos de gestión de incidentes y sus equipos de desarrollo sean capaces de volver a la normalidad en horas.

No creo que exista un único protocolo de role back. Cada proveedor tendrá sus propios mecanismos preventivos y reactivos, y no se activarán el día que se produzca el incidente, están permanentemente activados. Como dicen en uno de ellos, "todo lo que puede fallar, fallará, diseña los servicios teniendo en cuenta que todo va a fallar en algún momento".

¿Pueden las pymes, con recursos limitados, incurrir en el modelo Cloud?

Deben. El modelo Cloud se ajusta todavía más a una pyme que a una gran empresa.

Es extremadamente difícil que una pyme no tecnológica pueda obtener una ventaja competitiva del uso de la tecnología básica (ERP, CRM, productividad personal, etc). Si alguien proporciona esos servicios con unos KPIs razonables a un coste razonable, no hay debate.

Lo más importante para una pyme es maximizar el foco en su negocio y explotar su ventaja competitiva, la Cloud permite incrementar ambos.

¿Qué carencias existen a nivel regulatorio para la Cloud?

Los grandes proveedores de IaaS, PaaS y SaaS están invirtiendo grandes cantidades de dinero en satisfacer las distintas regulaciones. Sus economías de escala les permiten obtener rápidos y grandes retornos de esas inversiones.

Los esfuerzos regulatorios para las organizaciones individuales no tienen sentido, erosionan sus márgenes para poder seguir en su actividad.

Es evidente que las combinaciones de geografías (más de 150 países) y sectores (más de 12-14 verticales) dificultan el cumplimiento regulatorio para los proveedores de Cloud, pero en cualquier caso considero que son más eficientes que cualquier organización individual.

Los expertos hablan de una revolución de la Cloud que generará una verdadera transformación digital, ¿es el Edge el nuevo centro de atención?

La Cloud ya ha acelerado la transformación digital. Sería posible cuantificar cuánto la ha acelerado en empresas concretas, en sectores verticales y agregando incluso en regiones o países. Posiblemente, en el año y medio de pandemia se han dado más pasos en la transformación digital que en una situación de normalidad.

La construcción de la Cloud pública actual no puede garantizar el procesamiento en tiempo real en su definición formal. Las nuevas tecnologías de comunicaciones, 5G por ejemplo, posibilitan nuevos servicios en "casi tiempo real". Por las latencias de red, no tendría sentido que muchos de esos datos viajaran a los grandes centros de datos de los CSPs. Esta situación ha obligado a implementar el concepto de Edge (que no es nuevo), para algunos servicios el Edge es una obligación, para otros muchos no tiene sentido.

En tu opinión, ¿consideras que la Cloud puede ser un elemento estratégico para el desarrollo de negocio?

Los negocios estacionales tienen un gran aliado en la Cloud si la consumen adecuadamente.

Los negocios con franjas temporales de consumo muy poco homogéneas tienen un gran aliado en la Cloud si la consumen adecuadamente.

Los equipos humanos de negocio con gran capacidad de hacer procesos de cómputo de prueba y error tienen un gran aliado con la Cloud.

Hay negocios que son viables económicamente gracias a la Cloud. Hay otros negocios que pueden ganar puntos de rentabilidad gracias a la Cloud.

Algunas actividades muy regulares, muy predecibles, con grandes barreras de entrada, pueden no encontrar ninguna ventaja competitiva real usando la Cloud.

Estos diagnósticos deben ser realizados en los Comités de Dirección, al más alto nivel, y actuar en consecuencia.

FIRMA INVITADA

BERNARDO CRESPO

Director Académico del Programa Executive en Transformación Digital en IE Business School.

It's the data, stupid

Cómo migrar hacia un entorno de Data TRUST-formation

Bernardo Crespo es Director Académico del Programa Executive en Transformación Digital en IE Business School.. También es miembro del Consejo Digital de IE Executive Education (IE Digital Advisory Board).

Actualmente combina la labor docente con la labor inversora en proyectos intensivos en Inteligencia Artificial, Blockchain y proyectos con foco en generación de talento digital. Ha sido Director de Marketing Digital en BBVA España y Digital Transformation Leader en Merkle - Spain, y ha sido reconocido por el diario EXPANSIÓN en 2016 como uno de los 50 mayores expertos sobre Transformación Digital en España.

«La economía, estúpido»

James Carville

Esta frase de James Carville dominó la campaña presidencial en Estados Unidos en 1992, llevando a la Casa Blanca a Bill Clinton en detrimento de su adversario–George H. W. Bush. ¿Es posible que casi tres décadas más tarde tengamos que cambiar la frase para explicar el contexto actual?

ARTÍCULO

Quizás nunca pensamos que el dato fuera el recurso más valioso del planeta, incluso superando al petróleo. Y hoy en día es el caso. De otro modo nunca sería explicable que una empresa pagara multiplicadores desproporcionados sin tener en cuenta ingresos o beneficios y tan solo teniendo en cuenta usuarios activos diarios o mensuales. **Facebook** desembolsó en líquido y acciones 16.000 millones de dólares por **Whatsapp**, una empresa que no tenía ingresos (no hablemos de beneficios). Se estima en 55 dólares por usuario aquella adquisición en febrero de 2014.

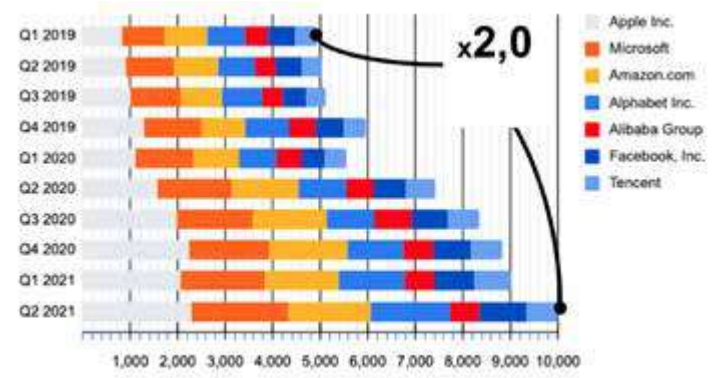
Del mismo modo, **Google** adquirió **Fitbit** por 2.100 millones de dólares en julio de 2019. Una empresa que había dado pérdidas en los ochos trimestres anteriores de forma recurrente. Y **Salesforce** ha completado este mes de julio de 2021 su adquisición de **Slack** por la friolera de 27.700 millones de dólares, en este caso una plataforma de comunicación / integración / colaboración empresarial con más de 100.000 usuarios de pago, y sin embargo, Salesforce ha pagado más de 26 veces el valor de las ventas de la compañía, lo que representa aproximadamente un 2% del PIB de España. **¿Cuál es el valor intrínseco de esas compañías cuyas adquisiciones se traducen en porcentajes del PIB de los 20 países más ricos del mundo?**

Datos. Información. Potencial de creación de valor adicional al hacer uso de esos datos. El dato es el mayor racional para explicar desproporcionados fondos de comercio. Y esas operaciones nunca las calcula un ingeniero en solitario, estamos hablando de negociaciones entre financieros con entendimiento de las posibilidades del dato y la tecnología: *"It's the data, stupid"*.

De hecho, hoy en día, inmersos en el reto de la sostenibilidad, nunca bautizaríamos al petróleo como el "oro negro". Quizás le llamaríamos (en caso de seguir siendo el petróleo el recurso más valioso del planeta) el "numérico negro" o el "dato negro". Y quizás de "dato negro" es de lo que verse la conversación sobre el futuro distópico de una deriva planetaria en la que el nuevo oro, el nuevo petróleo, es el causante de desarticular democracias y de hacer que las siete empresas más valiosas del planeta sean las que mayor acopio de datos hacen hoy en día a diario. Y lo siguen haciendo mientras lees estas líneas. Apple Inc., Microsoft, Amazon.com, Alphabet Inc., Facebook, Inc, Tencent, y Alibaba Group han multiplicado su valor en bolsa de 4.924 millones de millones de dólares USA ($4.9 trillions) en el primer trimestre de 2019 a 10.064 a finales del segundo trimestre de 2021 ($10.1 trillions). Por ponerlo sencillo, x2 en 2 años y pico.

Con una penetración de Internet cercana al 60% en todo el planeta y donde el dispositivo móvil representa el 91% del tráfico en Internet, hoy en día podríamos decir que la humanidad es el sumatorio de casi 7.883 millones de seres humanos (personas) conectados por una pléyade de dispositivos móviles (tecnología) y trazados de forma omnipresente en cada una de sus interacciones (datos). **Personas, datos y tecnología** son los pilares de una economía (digital) que algunos ya han bautizado como la era de la inteligencia artificial.

Somos personas trazadas que conviven



Fuente: Elaboración Propia @b_crespo a partir de Wikipedia

con la tecnología en un entorno donde la incertidumbre es el nuevo impuesto indirecto que toca aceptar para dirigir nuestras vidas. **¿Podemos reclamar que se limite el poder de aquellas empresas que han trazado nuestras vidas o podemos hacer apología de la propiedad sobre esa minúscula pieza de información que se ha convertido en el activo más valioso del planeta?** Y lo cierto es que desde que se creó la red global de conexiones que llamamos Internet, todos hemos caído atrapados en un espacio de conversaciones e intercambios de un valor incalculable. Esta red ha derivado en el hecho de que el código que la soporta y su capacidad de trazar **son las personas y sus actos trazables el activo más valioso**. Y el hecho de que gracias al código que soporta esa red, nuestros actos cotidianos se conviertan en más código, que a su vez genera aún más código y más aprendizajes, y esa es la única razón por la que el dato es la conversación que debe dirigir el debate para construir un futuro más sostenible para nuestra humanidad. Si rompemos la confianza por un mal uso de la tecnología y los datos, crearemos una deriva distópica que ninguno de nosotros desea, aunque la hayamos visto ya reflejada de forma brillante en algunas series.

Por lo tanto, quizás el dato no sea el nuevo petróleo, de hecho, no lo es *stricto sensu* al no ser un recurso limitado que puede ser recolectado, almacenado, compartido y vuelto a usar sin perder su valor (y cito a Margrette Vestager). Nos toca diseñar colaborativamente espacios sostenibles en los que la confianza sea la única moneda no negociable. Y en la era de la Inteligencia Artificial como reza la vicepresidenta ejecutiva responsable de la cartera de una Europa Adaptada a la Era Digital:

«En cuanto a la inteligencia artificial, la confianza es una obligación, no un adorno»

Margrette Vestager

El dato es la conversación que debería estar ocupando la agenda de todos los gobernantes de este planeta, por encima del dinero, la tecnología o los votos. El dato cambia la opinión de las personas y altera los resultados de las elecciones. El dato permite optimizar el uso que hacemos de nuestros ubicuos dispositivos móviles. Y en definitiva, el dato es el que permite inferir aprendizajes ocultos de seres que un día fueron libres antes de la invención de Internet. ¿Quedan dudas de por qué es el activo más valioso del planeta?

DATA TRUST-FORMATION: ¿CÓMO ENTENDER EL RETO DE CONSERVAR LA INFORMACIÓN DE FORMA CONFIABLE?

La seguridad de la información no puede ser responsabilidad de una sola persona en nuestras organizaciones, al igual que la transformación digital no puede recaer sobre una única posición.

Conservar y mantener la información nos ha llevado a la búsqueda y mitigación de riesgos en el acceso a los datos por parte de personas no autorizadas. Regular la conservación de la información parece invitarnos de forma inconsciente solo a anticipar riesgos. Por ende, volver nuestro foco hacia la seguridad.

Quizás sea una óptica parcial. Al igual que proteger la privacidad desde el lado de la propiedad de la información es una óptica limitada. **Nuestra información ha dejado de ser nuestra porque a diferencia de cualquier otro activo, nuestros datos se pueden multiplicar exponencialmente conservando su valor**. Mi email o mi número de teléfono móvil hoy en día están en miles, quizás decenas de miles de repositorios de datos de los cuales yo no tengo constancia. Por lo tanto, regular la propiedad del dato es algo tan cercano a la estulticia como definir quién es el propietario de las moléculas de oxígeno que respiramos a diario.

La seguridad de la información debe ser una responsabilidad compartida por todos los stakeholders de una compañía y no puede recaer únicamente sobre la figura del CISO. La protección y la conservación de la información es una tarea colaborativa. El pasado 4 julio tuve la oportunidad de estar con muchos de vosotros en el cierre de unas jornadas de ISMS Forum y tuve la osadía de renombrar el literal de su función. De responsables de la seguridad de la información, a responsables de la confianza en el uso de la información en un entorno de transformación. **De CISOs a responsables de Data Trust-formation**. Hace tiempo que todos hemos entendido que la transformación digital debe tener su foco en generar entornos de confianza: Digital TRUST-formation.

The Economist. Front Cover May 6th-12th, 2017

Un CISO debe ser el responsable de conservar la confianza en el uso de la información. Y puesto que la confianza, por definición, es una emoción que se construye sobre acciones iterativas de múltiples individuos, no puede recaer sobre una sola persona. Si no concienciamos a nuestras organizaciones sobre el uso confiable de la información, estaremos creando un

puesto orientado a la minimización de desastres (proteger la seguridad) y no a la estabilidad, sostenibilidad y confiabilidad en el uso de la información.

El reto del CISO está posiblemente más cerca del Chief Data Officer de la compañía y quizás menos cerca del Chief Information Officer. Incluso más cercano a cualquier puesto a primer nivel donde la comunicación (CCO) y la formación (CHRO) sean palancas de acción. Y todo con el objeto de crear dinámicas que generen confianza en la organización, y, huir de recomendaciones catastróficas que siembran el miedo y minan la credibilidad de CISO.

Proteger la confianza quizás sea la mejor forma de prevenir vulnerabilidades en el acceso a los datos. La estrategia de datos de una compañía tiene dos posibles enfoques: uno defensivo y otro ofensivo. Desde la óptica defensiva, mejorar el uso, la optimización de procesos y la seguridad de la información; y desde la óptica ofensiva, utilizar los datos como palanca para la transformación y la generación de valor. Aunque entendamos que naturalmente la función del CISO tradicional está en la defensa, estamos errando el tiro si pretendemos construir confianza de forma defensiva.

Mi recomendación es acercar la función del CISO a la de un constructor de confianza en el uso de la información. En el fondo todos somos jugadores de un equipo que pretende generar confianza en contextos de incertidumbre donde lo digital es una realidad. A modo de lista, dejadme que resuma la visión estratégica:

- Fomentar la confianza en el uso y acceso a la información de toda la compañía.
  Fomentar una serie de prácticas tendentes a generar confianza y "accountability" en todos los usuarios.

- Traducir mitigación a generación de valor de forma conjunta con el responsable último del dato en la compañía.

- Crear entornos de confianza y corresponsabilidad en el uso de la tecnología como puerta de acceso a la información.

- Educar, enseñar y promover la necesidad de preservar la seguridad en la recolección, transporte y procesamiento de la información a todos los usuarios de la organización.

- Promover la colaboración entre compañías para generar ecosistemas interoperables más resilientes y trazables.

- Y en última instancia, liderar entornos de crisis (no deseados, cuando fuera necesario) minimizando el impacto de un daño, que tristemente, ya está hecho.

Prohibir, alertar, asustar quizás sean máximas de un viejo enfoque sobre la figura del CISO tradicional. Ahora toca educar, compartir, enseñar y facilitar la confianza. Y quizás esta visión no se consiga en un solo día.

«El consejo es como la nieve: cuanto más suave cae, más tiempo permanece y más se hunde en la mente»

Samuel Taylor Coleridge

PROYECTOS DE INTERÉS

ISMS Forum y Cloud Security Alliance España publican el XI Estudio del Estado del Arte de Seguridad en la Nube

El ISMS Forum -International Information Security Community-, junto a la Cloud Security Alliance España, publica el IX Estudio del Estado de la Seguridad en la Nube, en el marco del XI Encuentro de Cloud Security Alliance España 2021.

Este estudio continúa la serie de estudios sobre el Estado del Arte en la Seguridad de los Servicios en la Nube que se vienen desarrollando desde el año 2013, y busca investigar y conocer el Estado del Arte de la adopción de la Computación en la Nube, así como el papel que juega la seguridad en la adopción de estos servicios. Todo ello, desde el punto de vista de los Usuarios de Servicios en la Nube.

Para ello, este 9º Estudio del Estado del Arte de Seguridad en la Nube trabaja en un triple eje:

- En primer lugar, esta edición del Estudio se ha desarrollado durante la pandemia de Covid19. Por ello, se ha analizado el impacto de la Covid19 en las organizaciones, en sus operaciones y en el uso de soluciones en Nube para articular en las organizaciones respuestas a la nueva normalidad derivada de la pandemia.

- En segundo lugar, el Estudio analiza las diferencias entre dos tipologías de usuarios de la Nube: usuarios finales, que habitualmente demandan servicios estandarizados pero que no tienen un conocimiento técnico profundo; y usuarios técnicos, que conocen y dominan en detalle las tecnologías en que se soporta la Nube y por ello demandan tanto servicios estandarizados como servicios más especializados y específicos de sus organizaciones.

- Por último, el estudio prolonga las líneas de investigación clásicas del estudio: expectativas, requisitos y satisfacción de los usuarios con los servicios recibidos de su proveedor de servicios en la Nube, incidentes en los servicios, y concienciación de los usuarios o ShadowIT.

Consulta la nueva versión de la "Guía para la notificación de brechas de datos personales" de la AEPD

La "Guía para la notificación de brechas de datos personales" es un documento que tiene como objetivo guiar a los responsables de los tratamientos de datos personales en su obligación de notificarlas a las autoridades de protección de datos y comunicárselo a las personas cuyos datos se hayan visto afectados. Esta guía actualiza la versión publicada en 2018, cuando comenzó a aplicarse el Reglamento General de Protección de Datos (RGPD), e incluye la experiencia recogida en este tiempo, tanto a nivel nacional como en relación con los criterios establecidos por el Comité Europeo de Protección de Datos.

El principal propósito de esta actualización es facilitar el cumplimiento de forma eficaz y eficiente de los objetivos últimos de la notificación de brechas de datos personales: la protección efectiva de los derechos y libertades de las personas, la creación de un entorno más resiliente basado en el conocimiento de las vulnerabilidades de la organización y la garantía de una seguridad jurídica al disponer los responsables de un medio para demostrar diligencia en el cumplimiento de sus obligaciones.

La Guía comienza analizando qué es una brecha de datos personales y qué no lo es en el contexto del marco normativo europeo, nacional y sectorial. A continuación analiza cuándo hay que notificar dicha brecha a la autoridad de control, en qué plazo, o quién y qué contenido debe incluir esa notificación. En lo relativo a la comunicación a las personas afectadas, el documento recoge en qué casos hay que realizarla, el contenido y sus plazos.

Las notificaciones y comunicaciones relativas a brechas que afectan a datos personales forman parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla o comunicarla no implica necesariamente la imposición de una sanción. De hecho, hacerlo en tiempo y forma es una evidencia de la diligencia de la organización, mientras que no cumplir con esa obligación sí está tipificado como infracción.

Ya está disponible la "Guía de Gestión de riesgo y evaluación de impacto en tratamientos de datos personales" de la AEPD

El documento incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos.

La Guía está dirigida a responsables, encargados de tratamientos y delegados de protección de datos (DPD). Ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

El RGPD establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de establecer las medidas que sean necesarias para garantizar los derechos y libertades de las personas. Además, en aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el Reglamento dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos (EIPD) para mitigar esos riesgos.

La Guía es aplicable a cualquier tratamiento, con independencia de su nivel de riesgo. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la EIPD y, en su caso, la consulta previa a la que se refiere el artículo 36 del RGPD, que establece que el responsable debe consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto sigue ofreciendo un riesgo residual alto o muy alto tras haber tomado medidas.

La Guía consta de tres apartados: el primero contiene una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades; el segundo incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo, y el último está enfocado en los casos en los sea preciso realizar una EIPD, con las orientaciones necesarias para llevarla a cabo.

CSA-ES, junto con los capítulos de Bolivia, Chile y Perú, traduce al español la Cloud Controls Matrix v4

Cloud Security Alliance España en colaboración con los capítulos de Bolivia, Chile y Perú ha traducido al español la nueva versión (v4) de la matriz de controles de referencia para la seguridad Cloud. El objetivo principal de la creación de una versión en español de la última versión del Cloud Controls Matrix es impulsar la adopción de servicios de Cloud en España, permitiendo tanto el cumplimiento normativo como la seguridad efectiva de los datos.

CCM es el esquema de controles de ciberseguridad que se alinea con las mejores prácticas de CSA y es considerado el estándar de facto para la seguridad y privacidad en la Nube. CCM v4 constituye una actualización significativa en relación con la versión anterior (v3.0.1). Incluye 17 dominios y un total de 197 controles. Asimismo, se ha traducido el mapeado de sus controles con CCM v3.0.1 y con las ISO/IEC 27001/27017/27018.

Una vez se apruebe la nueva versión del Esquema Nacional de Seguridad (ENS) Cloud Security Alliance España iniciará los trabajos para incluir el mapeado del ENS con CCMv4.

La Comisión Europea propone la creación de una unidad informática conjunta

La Comisión presentó el pasado junio una nueva visión para construir una unidad informática conjunta con el objetivo de hacer frente al creciente número de ciberincidentes graves que afectan a los servicios públicos y a la vida de las empresas y los ciudadanos en toda la Unión Europea.

La unidad informática conjunta tiene por objeto reunir los recursos y la experiencia de que disponen la UE y sus Estados miembros para prevenir, disuadir y responder eficazmente en materia de cibercrisis y ciberincidentes masivos. Las partes interesadas en la ciberseguridad, incluidas las del mundo civil, policial, diplomático y de ciberdefensa, y los socios del sector privado suelen trabajar demasiado a menudo por separado. Gracias a la unidad informática conjunta, contarán con una plataforma virtual y física de cooperación: las instituciones, órganos y organismos pertinentes de la UE, en colaboración con los Estados miembros, crearán gradualmente una plataforma europea de solidaridad y asistencia para luchar contra los ciberataques a gran escala.

accenture
Aiuken Cybersecurity
Akamai
aruba
a Hewlett Packard Enterprise company
cipher
CISCO
CLOUDFLARE
CROWDSTRIKE
DEVO
fastly
FIREEYE
FORCEPOINT
SIA
helpsystems
Tech solutions. Human support.
HUAWEI
IBM
OneTrust
paloalto
PCYSYS
proofpoint
riskrecon
NETWITNESS
An RSA Business
S21SEC
SAMSUNG
splunk>
tenable
thycotic
transmit
SECURITY

GLOBAL

BeyondTrust
BITSIGHT
Capgemini
Check Point
CYTOMIC
DARKTRACE
deepinstinct
Deloitte.
FORESCOUT
ForgeRock
FORTINET
f5
McAfee
Microsoft
netskope
NEXTVISION
SecurityScorecard
Qualys.
radware
Recorded Future
retarus
SECURONIX
SentinelOne
SKYBOX SECURITY
SOPHOS
TREND MICRO
VARONIS
VECTRA
vmware
zscaler

SPONSORS

ISMS Forum - International Information Security Community, es una organización sin ánimo de lucro que promueve el desarrollo, conocimiento y cultura de la Seguridad de la Información en España. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información.

915 63 50 62

info@ismsforum.es

Calle Segre 29, 1B
28002, Madrid, Spain

@ISMSForum

ISMS Forum