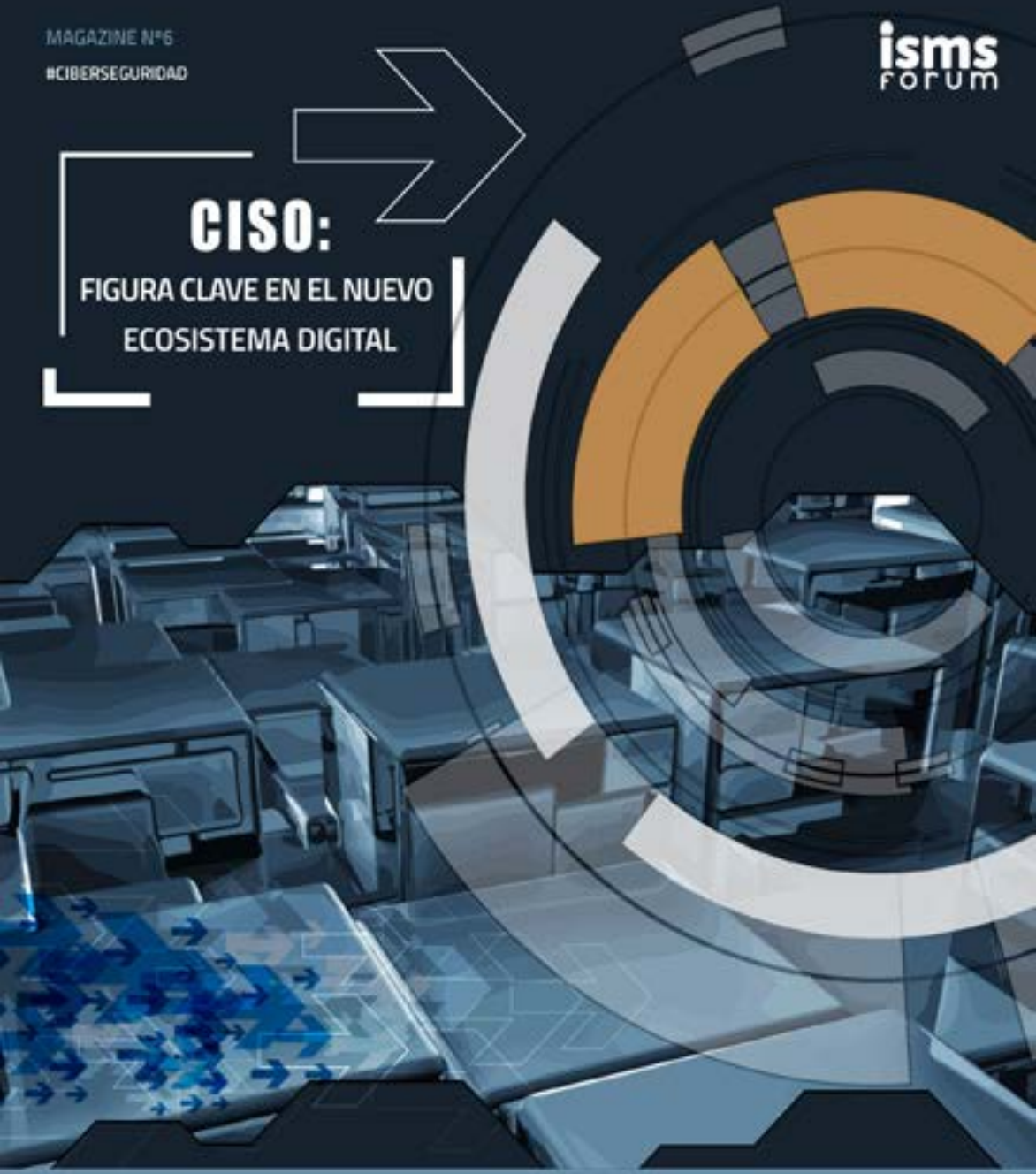
MAGAZINE Nº6

#CIBERSEGURIDAD

CISO:

FIGURA CLAVE EN EL NUEVO ECOSISTEMA DIGITAL



El Magazine semestral de ISMS Forum - International Information Security Community

ENTREVISTAS

"El CISO va a elevar de nuevo su función, o al menos verse integrado en roles de alta dirección con visión transversal y no solo técnica o digital"

ROBERTO BARATTA

Director of Loss Prevention, Business Continuity and Security, and DPO, Abanca; Board member, ISMS Forum.

FIRMA INVITADA

El arancel digital oculto de la ciberseguridad en la transformación digital

DANIEL LARGACHA

Cyber Security Centre Director, ISMS Forum; Global Control Center CERT Assitant Director, Mapfre.

ACTUALIDAD

La App de ISMS Forum que necesitas se hace realidad

REDACCIÓN ISMS FORUM

FEBRERO 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

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

UN CAFÉ CON LOS EXPERTOS

ROBERTO BARATTA

Director of Loss Prevention, Business Continuity and Security, and DPO, Abanca; Board member, ISMS Forum

"El CISO va a elevar de nuevo su función, o al menos verse integrado en roles de alta dirección con visión transversal y no solo técnica o digital"

IVÁN SÁNCHEZ

CISO, Sanitas; Board member, ISMS Forum

"Una vez transpuesta la NIS2 podemos esperar un régimen sancionador más elevado al actual"

JOSÉ RAMÓN MONLEÓN

CISO, Orange; Board Member ISMS Forum

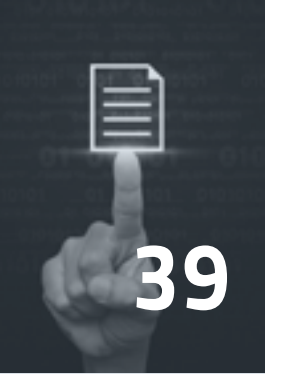
"Los operadores van a realizar fuertes inversiones y necesitan certidumbre a la hora de invertir"

FIRMA INVITADA

DANIEL LARGACHA

Cyber Security Centre Director, ISMS Forum; Global Control Center CERT Assitant Director, Mapfre

El arancel digital oculto de la ciberseguridad en la transformación digital



PROYECTOS DE INTERÉS

Conoce a los ganadores de la II Edición de Emprendimiento e Innovación de ISMS Forum.

El Observatorio de Ciberseguridad de ISMS Forum Barcelona lanza el Indicador de Madurez en Ciberseguridad.

Consulta la Guía para la gestión de crisis por ciberincidente en la cadena de suministro.

GAZINE

CARTA DEL PRESIDENTE

Consolidando el rol profesional del CISO

GIANLUCA D'ANTONIO

Presidente de ISMS Forum

ismsforum.es

Estimados profesionales de la seguridad de la información y socios de ISMS Forum:

No puedo ocultar mi satisfacción mientras escribo estas líneas para presentar el próximo número de nuestro Magazine semestral considerando que el pasado jueves 28 de enero se publicó en el BOE el Reglamento de Desarrollo de la Ley NIS (Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información). Algo que muchos esperábamos desde hace tiempo y que, sin lugar a duda, ayudará a desarrollar y consolidar la practica de seguridad de la información en las organizaciones que operan en España.

Este Real Decreto disciplina aspectos relevantes de los sistemas la gestión de la seguridad de la información para los Operadores de Servicios Esenciales así como de sus proveedores de servicios digitales.

Habrá tiempo para analizar y comprender todas las derivadas de los artículos 6 y 7 del Reglamento que establecen las medidas de seguridad y definen la función del Responsable de Seguridad de la Información así como de su equipo. Seguramente habrá quien opinará que se hubiera podido aprovechar la ocasión para profundizar más en las obligaciones de los operadores o en los requisitos profesionales del Responsable de Seguridad de la Información.

Yo soy de los que prefieren avances graduales pero constantes, soy de los que se conforman con una buena norma en lugar de la regla perfecta, soy de los que suscriben la afirmación de Platón, cuando el filósofo decía: "No conozco el camino seguro para el triunfo, pero si el camino para el fracaso; el querer complacer a todo el mundo".

ACTUALIDAD

ISMS FORUM

ACTUALIDAD

ISMS Forum incorpora el derecho digital entre sus dominios de trabajo

Redacción ISMS Forum

ISMS Forum -International Information Security Community- establece una alianza con ENATIC, la asociación que aúna a los profesionales de la Abogacía Digital, con el objetivo de compartir y difundir sus conocimientos de manera conjunta.

Ambas asociaciones han establecido un Plan de Acción Estratégica que supone grandes sinergias a medio y largo plazo, centrando el círculo de ciberseguridad y protección de datos con las consideraciones sobre derecho digital. El objetivo de esta alianza es generar contenidos y actividades de interés para ambos públicos.

En esta línea, ISMS Forum y ENATIC han puesto en marcha un grupo de trabajo con la finalidad de explorar estas sinergias en materia de ciberseguridad, riesgos digitales o privacidad, así como establecer acuerdos que permitan a los asociados de ambas asociaciones contar con mayores facilidades para participar en actividades colaborativas, formaciones y congresos.

Recientemente, Carlos A. Saiz, Presidente de ENATIC, Vicepresidente de ISMS Forum y socio de Ecix Group, comentó en una entrevista para *Abogacía*: "una asociación como ENATIC tiene que ser activa en el debate público de la repercusión jurídica y en los derechos que tiene el desarrollo de las tecnologías desde todos los puntos de vista; representar a la Abogacía digital y participar con criterio experto ante el desarrollo del marco normativo del Estado que nos viene en los próximos años en asuntos tan trascendentales como los derechos digitales, la seguridad de las redes, el data governance, la protección de alertadores, el trabajo a distancia, los planes estratégicos de ciberseguridad, etc; y debe promover la preparación, sofisticación y especialización de abogados digitales y ciberabogados". Desde ISMS Forum, nos sumamos a esta iniciativa con el fin se seguir ejerciendo nuestra labor de concienciación y divulgación de la seguridad de la información desde otras áreas de trabajo relacionadas con las que actualmente abarca.

La App de ISMS Forum que necesitas se hace realidad

Redacción ISMS Forum

ISMS Forum lanza su propia App pensada para que tengas las novedades del sector de la ciberseguridad y protección de datos en un mismo sitio: últimas noticias, estudios, documentos y actividades relacionadas con las temáticas de ciberseguridad, privacidad, movilidad e IoT, Cloud y Continuidad de negocio, entre otras.

¿Por qué descargar nuestra App?

- Podrás seleccionar tus temas de interés y recibir información actualizada sobre ellos en todo momento. Serás el primero en estar al tanto de contenidos de calidad, esos que antes tenías que buscar y a partir de ahora encontrarás sin hacer nada.

- También podrás guardar tus noticias favoritas para tenerlas a mano, leerlas más tarde cuando tengas tiempo y acceder a ellas siempre que quieras.

- Contarás con una agenda que reúne las fechas de todos nuestros eventos, formaciones y convocatorias de exámenes de certificación que preparamos durante todo el año. Apúntate a golpe de clic y añádelos a tu calendario.

- Descarga contenido como vídeos, fotografías de eventos y estudios, tanto exclusivos de ISMS Forum como externos, que constituyen documentos de referencia y de lectura imprescindible para todo profesional y experto en Seguridad de la Información.

- Además, si eres socio de ISMS Forum, tendrás acceso exclusivo a promociones y descuentos de los que podrás aprovecharte y que la Asociación quiere ofrecerte por ser parte de nuestra comunidad. Y si aún no eres socio, tendrás acceso directo para hacerlo y descubrirás cuáles son las ventajas de ser parte de nuestra familia.

- Recuerda aceptar los permisos para recibir notificaciones push y seleccionar tus preferencias al inicio, así podrás disfrutar del contenido de tu interés y recibir alertas para no perderte un solo detalle.

¿A qué esperas?

No te quedes fuera y regístrate en la que ya es y será la App de referencia en el sector.

Encuéntranos en

Download on the App Store

ANDROID APP ON Google play

CRÓNICA

Shaping a Sustainable & Disruptive Digital Risk Strategy

CRÓNICA

La Estrategia Digital a debate: "Cuando nos atacan no podemos emplear nuestro tiempo en discutir si pagamos o no"

Redacción ISMS Forum

El ISMS Forum celebró su XXII Jornada Internacional de Seguridad de la Información el pasado 26 de noviembre en modalidad online, bajo el título Shaping a Sustainable & Disruptive Digital Risk Strategy, haciendo referencia a la necesidad de crear una verdadera estrategia digital que permita generar la estabilidad que el negocio necesita. Más de 800 profesionales se reunieron en torno a cuatro Tracks con más de 30 ponencias, y con la presencia de más de 70 ponentes de primer nivel que compartieron las claves para afrontar los nuevos escenarios que se presentan desde el punto de vista de la ciberseguridad y la protección de datos.

La Sostenibilidad como eje central de la ciberseguridad

La primera ponencia que dio cuerda a este encuentro fue la de Troels Oerting, Chairman of the Advisory Board, Centre for Cybersecurity, World Economic Forum, que abordó la importancia del concepto de Sostenibilidad en el ámbito de la Ciberseguridad como piedra angular de la Estrategia Digital.

"Los ciberdelincuentes observan tres parámetros cuando deciden si quieren cometer un delito: cuál es la inversión, cuál es el riesgo y cuál es el beneficio, y en el ciberdelito tienes una inversión relativamente baja, un beneficio enorme y casi no tienes riesgo, así que, ¿por qué no continuar realizando ciberdelitos?", comentó el experto al inicio de su ponencia.

"He visto muchas pequeñas brechas que se han convertido en una gran crisis para una empresa porque se trataron mal desde el punto de vista comunicacional. Es necesario pensar en la resistencia antes, durante y después, se trata de predecir lo que va a pasar para poder prevenir y proteger nuestro estado. Por ello, es importante contar con un plan que nos guíe cuando sucede un incidente de seguridad. La clave es saber cuándo sucede, cómo lo detectas y cómo reaccionas, para poder aplicar el plan. Cuando nos atacan no podemos emplear nuestro tiempo en discutir si pagamos o no pagamos el rescate, tenemos que contar con una política empresarial, tanto si lo hacemos como si no, y saber de qué depende. Asimismo, debemos tener muy claro quiénes son los que formarán parte de nuestro equipo de gestión de crisis, quién se comunicará con la prensa, los accio-

Troels Oerting

nistas o los clientes, para asegurarnos de que podemos centrarnos en el problema principal sin tener que estar pendientes de otros problemas añadidos. Por eso debemos tener un plan de resiliencia para el antes, durante y después", declaró Troels sobre cuáles son los puntos a tener en cuenta a la hora de elaborar una Estrategia Digital.

El ponente concluyó su charla haciendo referencia a los nuevos ataques a los que nos enfrentaremos tras el paso de la COVID-19, "la pandemia también ha tomado a los cibercriminales por sorpresa, ahora se están preparando para la nueva normalidad y aún no hemos visto el resultado de eso. En el futuro podremos ver nuevos tipos de cibercrimen que aprovecharán la superficie de ataque que hemos creado después de la COVID-19 y tendremos que lidiar con ello, aunque también estoy seguro de que estamos mejorando y la ciberseguridad está pasando a ser una parte muy importante dentro de cada empresa".

En línea con el concepto de Sostenibilidad en el ámbito de la Ciberseguridad que desarrolló Troels Oerting, la Dr. Maria Bada, Senior Research Associate at Cambridge Cybercrime Centre, dedicó su intervención a hablar sobre el nivel de madurez en ciberseguridad como la clave para la sostenibilidad de la empresa.

La ponente se centró en el valor de los Key Performance Indicator (KPIs) para la mejora de la eficacia y productividad de las acciones que se lleven a cabo en un negocio con el fin de poder tomar decisiones y determinar aquellas que han

sido más efectivas a la hora de cumplir con los objetivos marcados en un proceso o proyecto concreto.

"Los indicadores clave de negocio nos ayudan a controlar o mitigar el impacto utilizando un enfoque de gestión de riesgos centrado en priorizar las situaciones con esta métrica de riesgo e indicar las medidas que deben adoptarse y, a continuación, sobre la base de los riesgos identificados, medir la eficacia de estos controles. Los KPIs muestran la historia de éxito o fracaso de la organización a la hora de tomar decisiones eficaces. El reto es saber identificar los criterios que son más aplicables a nuestra organización, ya sea una gran corporación o una pyme".

Perspectiva europea: el tratamiento de los datos y las transferencias internacionales de datos

En clave de privacidad, una de nuestras ponentes destacadas fue Karolina Mojzesowicz, Deputy Head of the Data Protection Unit, Directorate General for Justice and Consumers, European Commission, que habló sobre la transformación digital y la estrategia de datos europea.

"La comisión está trabajando muy intensamente en diferentes medios para abordar el programa y las herramientas necesarias que faciliten el intercambio de datos a través de la Unión Europea y entre diferentes sectores con el fin de crear riqueza y aumentar el control y la confianza tanto de los ciudadanos como de las empresas cuando compartan sus datos, así como para ofrecer nuestro modelo europeo a las prácticas de manejo de datos de las principales plataformas. Así pues, ¿qué aborda esta gobernanza de los datos? El Reglamento Europeo de Protección de Datos se refiere a un conjunto de reglas y medios para utilizar los datos, por ejemplo, a través de mecanismos de intercambio, acuerdos y normas técnicas, cada uno de los cuales implica estructuras y procesos para compartir los datos de manera segura, incluso a través de terceros", explicó Karolina.

El objetivo del Reglamento es crear las condiciones adecuadas para que las personas y las empresas confíen en que sus datos serán manejados por organizaciones de confianza basadas en los valores y principios por los que apuesta la Comisión Europea, "la Comisión tiene previsto invertir en torno a 2.000 millones de euros en el desarrollo de la arquitectura de los instrumentos, de las infraestructuras de procesamiento de datos y el mecanismo de intercambio de datos a través de los espacios de datos seguros", comentó la experta.

Por su parte, Ventsislav Karadjov, Deputy Chair, European Data Protection Board, expuso el punto de vista europeo de la privacidad desde el diseño y por defecto. "La European Data Protection Board elaboró en 2019 unas directrices que proporcionan orientación sobre la obligación establecida en el artículo 25 del Reglamento General de Protección de Datos. Estas directrices se han ultimado recientemente tras una consulta pública con las partes interesadas con el objetivo de desarrollar los conceptos de la

La protección de datos debe considerarse en una fase temprana y no puede ser solo una comprobación formal de última hora antes de iniciar el proceso de incorporación, por el contrario, tiene que ser parte integrante de todos los debates al desarrollar cualquier nuevo producto o servicio en todas las etapas del diseño.

privacidad desde el diseño y por defecto y marcar una orientación muy práctica para que el responsable del tratamiento pueda comprometerse a respetar la privacidad. Esto no solo ayuda a todos los responsables del tratamiento, sino que también sirve de guía para que las pequeñas y medianas empresas apliquen los requisitos en la práctica", declaró el experto.

Según Karadjov, "el Reglamento General de Protección de Datos es tecnológicamente neutro y no especifica ninguna medida para cumplir los requisitos de protección de datos desde el diseño y por defecto, por lo tanto, el controlador puede elegir las medidas más adecuadas según las circunstancias. Debe analizar, tomar medidas y rendir cuentas de esas medidas, por lo tanto ¿deberíamos conseguir que los fabricantes y los proveedores de software considerasen la protección de datos y la seguridad en la fase de diseño?, y ¿cómo sería esto posible? (...) la protección de datos debe considerarse en una fase temprana y no puede ser solo una comprobación formal de última hora antes de iniciar el proceso de incorporación, por el contrario, tiene que ser parte integrante de todos los debates al desarrollar cualquier nuevo producto o servicio en todas las etapas del diseño, de las actividades de procesamiento, incluidas las licitaciones de adquisición, la contratación externa, el apoyo al desarrollo, el mantenimiento, las pruebas de almacenamiento, etc.".

El ponente dedicó la última parte de su intervención a hablar sobre los procesos de certificación, "es importante saber que

Ventsislav Karadjov

la certificación es alentada por el RGPD, no es obligatoria, pero proporciona y agrega un valor añadido a un controlador en el momento de elegir entre diferentes bienes y servicios, ya que le sirve para demostrar que la protección de datos está incorporada en el ciclo de vida de su solución de procesamiento".

En esta dinámica, Leonardo Cervera, Director del European Data Protection Supervisor, abordó cómo el Reglamento General de Protección de Datos contempla las transferencias internacionales de datos. Para ello, puso de ejemplo la reciente sentencia Schrems II, por la que se invalida el Escudo de Privacidad, dejando de ser un mecanismo aplicable de manera inmediata desde la publicación de la sentencia para ofrecer garantías adecuadas en el caso de transferencias internacionales a empresas estadounidenses adheridas a este.

"El Escudo de Privacidad no garantiza un nivel de protección equivalente" declaró el experto, "debemos atender a un principio de responsabilidad proactiva, basado en catalogar las transferencias, revisar las herramientas, analizar el país tercero, identificar las salvaguardias adicionales y proceder a la suspensión de las transferencias si lo vemos conveniente" añadió.

Según Leonardo, "hay un antes y un después de la sentencia Schrems II, el problema sigue estando fuera de la Unión Europea y hay que tratar de relanzar la relación transatlántica, pero teniendo en cuenta que la responsabilidad es com-


Leonardo Cervera

partida, de los responsables de tratamiento y autoridades de control".

ISMS Forum lanza la Guía práctica para la gestión de riesgos de terceros en privacidad

La XXII Jornada Internacional de Seguridad de la Información sirvió como marco de referencia para el lanzamiento de uno de los últimos proyectos llevados a cabo por la Asociación, la Guía práctica para la Gestión de Riesgos de Terceros en Privacidad. Alfonso J. Menchén, Delegado de Protección de Datos en Iberdrola España, fue el encargado de presentar la Guía y los motivos por los cuáles se decidió desarrollar el proyecto.

El objeto de la Guía es establecer unas pautas generales, recomendaciones o buenas prácticas que permitan a las empresas concretar e implementar el principio general de la diligencia debida, especialmente a la hora de elegir a sus proveedores. Tras definir las obligaciones legales existentes, el documento aborda cuáles son las buenas prácticas según la fase en la que vaya teniendo intervención el proveedor: fase precontractual, fase contractual y fase de terminación de la relación contractual.

Otra de las ponentes destacadas de este encuentro fue Maite Boyero, miembro del Centro de desarrollo tecnológico industrial (CDTI) y principal enlace para el programa de Sociedades Seguras, integrado en el Programa Marco de la Unión Europea – Horizonte 2020, como representante de los intereses de España en dicho Comité, que participó con una ponencia bajo el título "La innovación y la ciberseguridad como capacidades de una Europa Digital".

"La Comisión está empezando a poner en marcha el desarrollo de la investi-

gación y la innovación para el período 2021-2027, será el próximo Programa Marco Horizonte Europa, el 9º Programa Marco para la investigación y la innovación en la Unión Europea cuyo objetivo es fortalecer el uso de la base científica y tecnológica en el área de investigación europea para impulsar la capacidad de innovación de Europa, la competitividad y el empleo, así como cumplir con las prioridades de los ciudadanos y mantener nuestros modelos y valores económicos y sociales", expuso la experta.

"Nuestros principales desafíos y aspectos clave se centran en mejorar la ciberseguridad en la transformación digital asegurando la autonomía estratégica en las herramientas tecnológicas de la ciberseguridad, así como las innovaciones en el desarrollo e implementación de hardware y software seguro, pruebas y certificación, prestando atención a la privacidad y seguridad desde el diseño en las tecnologías digitales y sus aplicaciones (5G, industria 4.0, IO, Blockchain, tecnologías cuánticas, dispositivos móviles y connectec movilidad y energía cooperativa y autónoma)", comentó Maite en relación a los objetivos perseguidos por el próximo Programa Marco de la Unión Europea.

"La pandemia de la COVID-19 ha puesto de relieve la necesidad de soluciones fiables y escalables"

Esta Jornada contó por primera vez con la presencia de Mario Beccia, Cyber Defence Officer, European Defence Agency (EDA), que abordó la temática de Ciberseguridad Transnacional. "El programa de defensa cibernética de la EDA incluye proyectos para hacer frente a desafíos como la conciencia de la situación cibernética, la protección avanzada contra amenazas persistentes, la ingeniería de sistemas para la defensa cibernética, la conciencia de la seguridad cibernética, el diseño de cursos de capacitación en defensa cibernética y muchos otros. La pandemia de COVID-19 ha puesto de relieve la necesidad de soluciones fiables y escalables que proporcionen comunicaciones fiables, ubicuas y seguras", declaró Beccia.

Asimismo, presentó el proyecto PESCO para la ciberdefensa, cuyo objetivo es desarrollar, establecer y poner en funcionamiento el Cyber and Information Domain (CID) Coordination Center (CIDCC) como elemento militar multinacional permanente, en el que -de conformidad con la resolución europea de 13 de junio de 2018 sobre la ciberdefensa- los Estados Miembro participantes colaboren continuamente con personal nacional pero decidan soberanamente, caso por caso, para qué amenaza, incidente y operación contribuyen con medios o información.

Sin duda, la XXII Jornada Internacional de Seguridad de la Información fue la cita ineludible de profesionales, expertos, compañías e instituciones públicas para debatir sobre el presente y el futuro que supone la Transformación Digital, la mejora constante de una Estrategia Digital que permita enfrentar los riesgos eficazmente y el tratamiento de los datos a nivel nacional e internacional, entre otros temas desarrollados.

UN CAFÉ CON LOS EXPERTOS

ENTREVISTAS

"El CISO va a elevar de nuevo su función, o al menos verse integrado en roles de alta dirección con visión transversal y no solo técnica o digital"

El pasado 24 de septiembre, la Comisión Europea publicó el borrador de Reglamento de Resiliencia Digital Operativa, (Dora por sus siglas en inglés -Digital Operational Resilience Act-) para el sector financiero. La propuesta forma parte del paquete de finanzas digitales, cuyo objetivo es seguir propiciando y apoyando el potencial de las finanzas digitales en términos de innovación y competencia, mitigando al mismo tiempo los riesgos que se derivan de ella. Está en consonancia con las prioridades de la Comisión de hacer que Europa esté adaptada a la era digital y construir una economía preparada para el futuro y al servicio de las personas. Este reglamento supondrá el establecimiento de un marco único europeo de obligaciones, principios y requerimientos en materia de ciberseguridad para el sector financiero.

¿Cuál es el objetivo de DORA y cuáles son, según su criterio, los principios más relevantes que incluye?

El Reglamento de Resiliencia Digital Operativa, (DORA por sus siglas en inglés -Digital Operational Resiliance Act-) es una iniciativa de la Comisión Europea a través de la Estrategia Digital Europea contenida en la Comunicación Shaping Europes Digital Future, el Next Generation Plan, y el Digital Finance Package. Implica el establecimiento de un marco único europeo de obligaciones, principios y requerimientos en materia de ciberseguridad del sector financiero considerado entre los estratégicos por la Comisión. Supone un nuevo enfoque de las actuaciones basado en el riesgo; la atribución de responsabilidad directa al consejo de administración sobre el establecimiento y cumplimiento de estrategias, políticas y protocolos adecuados; las nuevas responsabilidades del CISO; las políticas de identificación y clasificación de la información; la obligatoriedad de los planes de continuidad de negocio en caso de ciberataque; o las correspondientes estrategias de comunicación.

Con DORA en escena, ¿cómo cambia el modelo de gobierno de ciberseguridad en el sector financiero?

El giro no por obvio es menos relevante, ciberseguridad es una función y una responsabilidad transversal y vertical en una organización, pero también en su entorno. Es corporativa, es regulatoria y es personal, por lo que DORA profundiza en extender y definir con mayor claridad ese alcance. Y esto implica un tremendo foco en la gestión de terceros, la resiliencia digital como concepto de Continuidad de Negocio unida a Continuidad Tecnológica,

ROBERTO BARATTA

Director of Loss Prevention, Business Continuity and Security, and DPO, Abanca; Board member, ISMS Forum.

pero con el ámbito ciber como una de las mayores amenazas de disrupción de las operaciones y, por supuesto, la respuesta a incidentes y la compartición de la información, muy celebrada esta ultima por cierto, veremos cómo se plasma.

Una novedad que introduce DORA es un exhaustivo marco descriptivo relativo a los contratos con terceros suministradores tecnológicos. ¿Qué relevancia tienen estas medidas para vuestro sector?

La gestión de riesgos de terceros es algo que las organizaciones del sector venimos trabajando hace tiempo. El nivel de outsourcing y dependencia de terceros en entidades de base tecnológica y digital como son las financieras es alto y, por tanto, un marco de control y gestión de riesgo completo debe incluir el riesgo de terceros. Este camino ya fue iniciaco por el BCE (Banco Central Europeo) y la EBA (Europen Bank Authority) a través de instrumentos regulatorios como las Guidelines en cuestiones como Oustourcing y Cloud. Debemos esperar a ver cómo DORA integra o alinea estas normativas especificas del regulador sectorial, pero esta claro que el foco en terceros no va a dejar de crecer. A la vista está el numero y relevancia de ciberincidentes en proveedores tecnológicos y no tecnológicos en el año 2020, que han afectado en mayor o menor escala, al menos a nivel preventivo, a miles de compañías, entre ellas entidades financieras.

¿Qué opinas acerca del concepto de monitarización dinámica del riesgo?

En las entidades financieras estamos acostumbrados a la monitorización y ges-

tión del riesgo, al fin y al cabo es la esencia de nuestro negocio: confianza vs. riesgo. Los riesgos tecnológicos en general y la ciberseguridad en particular son riesgos de ciclo corto o ultra corto, esto significa que lo que no es un riesgo ahora puede serlo en una hora y dejar de serlo otra vez en varias horas. Un ejemplo: un descubrimiento de un zero-day en una tecnología clave de uso masivo supondría un riesgo alto una vez publicado, pero una vez dispongas de un parche y se verifique, deja de serlo. Este lapso son horas o días, en los que la exposición desde el punto de vista de riesgos es inmensa. Y es solo un ejemplo muy concreto. La monitorización dinámica lo que pretende es normalizar la forma de afrontar estos ciclos, cómo entrar en lo relevante para tu compañía, y cómo tomar esas decisiones de forma lo más ordenada posible en un entorno que cambia en minutos.

¿Cuál es su perspectiva sobre las nuevas políticas de identificación y clasificación de la información?

El encaje con el RGPD y las normativas de privacidad son clave. El impulso del RGPD a nivel europeo y la relevancia que la Comisión y demás reguladores presta a este ámbito impulsa e impulsará de forma radical la adopción de reglamentos y normas al respecto. El problema de la identificación y clasificación es siempre el modelo operativo y de gestión, cómo implantar estos mecanismos y controles que implica un equilibrio adecuado entre formación y concienciación de los empleados y controles técnicos. Nada es perfecto en esta implantación, es un modelo dinámico que cada organización debe elegir y ajustar, y

Los riesgos tecnológicos en general y la ciberseguridad en particular son riesgos de ciclo corto o ultra corto, esto significa que lo que no es un riesgo ahora puede serlo en una hora y dejar de serlo otra vez en varias horas.

El CISO tiene un rol clave en todo esto, de nuevo su perfil va a ser puesto a prueba, el rol técnico y de base operativa -me temo- está ya muy por debajo de las expectativas actuales y de lo que vienen. El CISO del 2022 de una entidad financiera es un alto directivo con cada vez más habilidades y funciones transversales que técnicas.

”

DORA pide expresamente eso: definirlo. Hay una clara convergencia por tanto entre las normativas encaminadas al cumplimiento normativo y seguridad de los datos.

¿Es posible que este reglamento suponga un impulso en términos de transformación digital a nivel global, ya que el sector financiero envuelve o implica a otros?

Esa es la idea por supuesto, DORA es un paso más en un camino iniciado con NIS, GDPR y PSD2, entre otras, para dotar a la Agenda Digital Europea de herramientas de gestión y control sobre los actores más relevantes en la Economía Digital, estrategia básica para Europa y contrapunto a la agresividad de las BigTech de origen estadounidense y chino. Obviamente la Comisión lo tiene sencillo: comencemos por sectores estratégicos como las Telco y el Financiero, por ejemplo, y por sectores que ya tienen mecanismos de supervisión y control muy maduros. Al final el despliegue normativo siempre empieza por el mismo lado, y las entidades financieras son perfectas para eso.

¿Qué implicaciones tiene esta nueva norma con respecto a la gestión de crisis y continuidad de negocio?

DORA aterriza una realidad que, no por obvia es sencilla de gestionar: las cosas pasan. Esta perogrullada se ha convertido en el leitmotiv de la Continuidad de Negocio de las entidades financieras, y de otras muchas, especialmente en el último año. Ciberincidentes y pandemias se han añadido a los problemas tradicionales de la operación: fallos, errores, rendimiento de la tecnología y lo digital cuya comple-

jidad es extrema y donde los terceros son parte clave, desde proveedores de tecnología hasta cloud, pasando por desarrollo de aplicaciones. Se trata de extender algo que en ciberseguridad es ya un mantra "invierte en detección y respuesta porque incidentes va a haber", incluyendo definir los sistemas y servicios core, escenarios de amenaza más relevantes, y preparar planes de contingencia y respuesta que incluyan a tus terceros clave.

¿El proceso de adaptación a las exigencias de DORA puede generar a los CISOs alguna controversia o inconveniente respecto a otras normas aplicables que ya lleva asumiendo el sector financiero? ¿Cuál es la mejor forma de adaptar esta norma en medio de la sobrerregulación que existe?

Es la tormenta regulatoria perfecta. Norma emanada de la Comisión, con un ámbito de gestión muy político y por ello con vaivenes y adaptaciones. Deberá integrar otras de origen similar como la NIS o el RGPD, y el regulador financiero ECB/JST/EBA, adaptar todo lo elaborado en estos ámbitos hasta ahora, incluyendo los mecanismos de valoración del riesgo tecnológico en los marcos de capital y solvencia. No hay una mejor forma de adaptarla que esperar a las directrices que vayan emanando de los diferentes reguladores. Se espera entre 18 y 24 meses para cerrar el borrador en el Parlamento y la Comision, y tiempos similares paralelos para adaptaciones en el regulador financiero. Bien es cierto que las bases ya están y se debe afrontar un gap análisis, al menos sobre la base normativa para definir aquellas áreas a mejorar y adaptar. El CISO tiene un rol clave en todo esto, de nuevo su perfil va a ser puesto a prueba, el rol técnico y de base operativa -me temo- está ya muy por debajo de las expectativas actuales y de lo que vienen. El CISO del 2022 de una entidad financiera es un alto directivo con cada vez más habilidades y funciones transversales que técnicas.

¿Tendrá que asumir el CISO responsabilidad ulterior como sus homólogos DPOs?

Totalmente, de una forma u otra la "accountability" va a llegar pronto. La responsabilidad de una entidad en la diligencia debida en ciberseguridad para evitar incidentes que afecten a sus clientes o a terceros se supone que está en manos del CISO, es la figura y se espera que asuma y gestione esa responsabilidad. Ya se están viendo demandas de unas compañías a otras por no haber dispuesto de medidas adecuadas en ciberseguridad y haber sido afectados por sus incidentes.

Por último, ¿supone entonces DORA un antes y un después para la consideración profesional o rol del CISO?

Desde luego, apunto ya que el CISO va a elevar de nuevo su función, o al menos verse integrado en roles de alta dirección con visión transversal y no solo técnica o digital. Cada organización debe definir un modelo, de forma similar a lo que está ocurriendo con los CIO: o elevo el rol del CISO con perfiles y funciones ya absolutamente transversales, o mantengo una función técnica pero reportando a niveles transversales donde se aúnen funciones que deben estar muy cerca de la Privacidad, Continuidad, Riesgo de Terceros, etc. La cuestión es: ¿estamos preparados? ¿existen ya estos perfiles senior ejecutivos?

"Una vez transpuesta la NIS2 podemos esperar un régimen sancionador más elevado al actual"

IVÁN SÁNCHEZ

CISO, Sanitas; Board member, ISMS Forum

El pasado 16 de diciembre de 2020 la Comisión Europea publicó la nueva estrategia de ciberseguridad, que tiene como objetivo reforzar la resiliencia europea contra las amenazas cibernéticas y garantizar la fiabilidad de los servicios digitales. Esta nueva estrategia incluye dos propuestas de directiva: la directiva de medidas para un nivel común de ciberseguridad en la Unión Europea (NIS2) y la directiva de resiliencia de entidades críticas. Uno de los principales avances incluidos en la NIS2 es abarcar más sectores que su predecesora, además, la propuesta elimina la distinción entre operadores de servicios esenciales y proveedores de servicios digitales, pasando a una clasificación basada en la importancia de las empresas; se dividen en dos categorías, esenciales e importantes, cada una de ellas sujeta a un régimen de supervisión diferente. Por otra parte, la propuesta aumenta los requerimientos de seguridad de las empresas, imponiendo un enfoque de gestión de riesgos y una lista de requerimientos básicos de seguridad.

¿De qué manera va a cambiar la NIS2 la definición de empresas que se consideran de carácter crítico y esencial?

Lo primero que me gustaría señalar es que la NIS2 supone un salto cualitativo y cuantitativo en las aspiraciones de la Unión Europea en materia de Ciberseguridad y resiliencia, y este es un mensaje muy positivo. Pero también hay que considerarlo como ambicioso, teniendo en cuenta el proceso tan complejo que supuso la trasposición de la Directiva NIS 2016/1148 original. En cuanto a los nuevos criterios de entidades en base a su importancia y divididos por categoría esencial o importante, tiene sentido teniendo en cuenta el incremento que desde 2016 ha habido en términos de digitalización y grado de interconectividad, así como por el propio hecho de que la directiva NIS original no recogía un gran número de sectores del ámbito digital que proporcionan servicios clave. Además, parece haber consenso por los profesionales de Ciberseguridad en este sentido, ya que uno de los puntos destacados tras el periodo de consulta pública de la propuesta fue el de la necesidad de la ampliación del alcance de la directiva a más sectores, para incluir por ejemplo a la Administración Pública o a entidades que prestan servicios de Data Center.

¿Qué papel va a tener de ahora en adelante el organismo supervisor que no se contemplaba en la primera NIS? ¿Cuáles son las medidas de supervisión que prevé la NIS2?

De los 3 objetivos fundamentales que persigue la NIS2, junto con el de una mayor cooperación y una gestión orientada al riesgo de Ciberseguridad, está el objetivo de aumentar las capacidades de supervisión. La NIS2 ahora va un paso más allá y faculta a las autoridades competentes de los estados para realizar tareas de supervisión adicionales con inspecciones on-site y off-site para entidades esenciales e importantes, añadiendo la capacidad de revisión aleatorias en entidades esenciales. Además, uno de los cambios principales que introduce es la capacidad que da a los estados de -en última instancia- aplicar sanciones que supongan la suspensión de la actividad de parte o de la totalidad de los servicios de una entidad esencial o incluso apartar (temporal o permanentemente) a personas físicas del ejercicio de sus funciones de dirección si estas no toman las medidas de gestión del ciberriesgo adecuadas. Creo que este es un caso muy extremo de la aplicación de la Directiva que espero no lleguemos a ver aplicado.

¿Cómo se han endurecido las normas y sanciones administrativas?

La directiva NIS original ya proponía a los estados la definición de un régimen sancionador en su trasposición a legislación nacional, si bien la propia Comisión Europea reconoce en su propuesta de NIS2 que "los Estados Miembro han sido reacios a aplicar sanciones a las entidades que no han puesto en marcha los requerimientos de seguridad". En el caso particular de España, la trasposición se tradujo en un rango de sanciones de 500.000 a 1m de euros en el caso de infracciones muy graves, pero sin haberse aplicado de manera efectiva. La nueva NIS2 parece querer ir más allá y dedica todo un capítulo para la definición de un modelo de

supervisión más exigente, con sanciones "proporcionales y disuasorias". Con todo esto, una vez transpuesta la NIS2 podemos esperar un régimen sancionador más elevado al actual. Aquí podríamos discutir largo y tendido sobre la efectividad de las sanciones para crear una dinámica positiva en términos de cumplimiento, si estas no van acompañadas de otras medidas.

La NIS2 contempla el establecimiento de una red europea de organización de enlace en crisis cibernéticas, denominada EU-CyCLONe, ¿este proyecto puede suponer una mejora en las capacidades de coordinación de esta crisis?

En la nueva NIS2, como decíamos antes, la cooperación es uno de los 3 objetivos fundamentales y va un paso más allá con la propuesta de creación de la "European Cyber Crises Liaison Organisation Network (EU - CyCLONe)" para la gestión y coordinación de eventos y ciberindicentes a gran escala, así como para el intercambio de información relevante entre estados e instituciones. La propuesta no es nueva, y de hecho la creación de esta red surge de la recomendación de la Comisión Europea 2014/1584 del 13 de septiembre de 2017, que hasta ahora no había tenido desarrollo. Sin duda creo que es un paso muy positivo, aunque falta ver aún algo más concreto de su implementación práctica ya que el articulo 14 de la propuesta de NIS2 apenas lo desarrolla

Según la NIS2, a partir de ahora habrá mayores requerimientos de seguridad con una lista de medidas de diversa índole, ¿supone esta directiva un cambio de paradigma en el modelo de gestión de riesgos?

Las regulaciones actualesse alejan cada vez más de un modelo de mero cumplimiento hacia un enfoque de gestión de riesgos y desde mi punto de vista es el enfoque adecuado, si bien es complicado una gestión de riesgos homogénea entre sectores tan diversos como los que abarca la nueva propuesta. En todo caso, y a falta de concretarse esos requerimientos, un aspecto positivo es que parece que vamos hacia una armonización de requerimientos y eso debería pasar por la definición de un framework de requisitos y de medición homogéneo. Un ejemplo en el que poder basarnos es en un modelo NIST "europeo" adaptado a la realidad de los diferentes sectores cubiertos por la directiva. Ahora bien, imaginemos que ese modelo que se define existe y es de aplicación obligatoria, lo siguiente es estimar el coste de implantación para las entidades, y ahí la propuesta ya nos da una idea en su anexo al estimar que "las compañías bajo el alcance de NIS se estima que necesitarían un incremento de un máximo de un 22% en su gasto actual en seguridad (un 12% en caso de que ya estén bajo la actual Directiva NIS)". En el contexto económico actual y con las perspectivas del futuro más inmediato no parece una tarea fácil, de manera que o bien estos incrementos se acompañan con algún tipo de estímulo económico o la implementación de ese modelo de requisitos de seguridad no llegará a tiempo.

¿Cuáles son las implicaciones más relevantes de la directiva en relación con la gestión de riesgos de terceros?

La primera de ellas es el propio reconoci-

miento de la importancia de los riesgos provenientes de terceros, y la necesidad de aumentar la supervisión a la hora de incorporar proveedores de servicios. De ahí se deriva que la nueva NIS introduzca la necesidad de cooperación entre autoridades nacionales, la Comisión y la ENISA para llevar a cabo revisiones sectoriales coordinadas en empresas proveedoras de servicios. Pero en este ámbito no solo la nueva NIS es relevante, ya que la gestión de riesgos de terceros es un aspecto aún más relevante de la propuesta 2020/0266 de la Comisión Europea para la resiliencia operacional, la conocida como DORA (Digital Operational Resilience Act), en este caso de aplicación al sector financiero. En general creo que veremos en los próximos años un foco cada vez mayor en la gestión de riesgos de terceros y de la cadena de suministro.

Por último, ¿qué valoración le merece la NIS2 y cómo cree que será el proceso de transposición de la directiva a España?

Como decía a principio, la NIS2 es un paso en la dirección adecuada en materia de armonización y mejora de la ciberseguridad a nivel europeo y puede llegar a suponer un cambio similar al que vivimos tras la entrada del vigor del RGPD. En España, la reciente aprobación del Real Decreto 43/2021 ya sienta una buena parte de las bases organizativas para su implantación, si bien el reto que tiene ahora la Comisión Europea es sacar adelante las negociaciones de la propuesta de NIS2 lo antes posible, teniendo en cuenta que posteriormente los estados tienen otros 18 meses para su trasposición nacional. No podemos perder tiempo en algo tan importante como asegurar el futuro de nuestras empresas y nuestra sociedad en el mundo digital.

Un aspecto positivo es que parece que vamos hacia una armonización de requerimientos y eso debería pasar por la definición de un framework de requisitos y de medición homogéneo.

"Los operadores van a realizar fuertes inversiones y necesitan certidumbre a la hora de invertir"

JOSÉ RAMÓN MONLEÓN

CISO, Orange; Board Member ISMS Forum

El pasado 14 de enero se cerró el periodo de audiencia pública del Anteproyecto de Ley de Ciberseguridad 5G. Esta norma establecerá los requisitos de ciberseguridad específicos para el despliegue y la explotación de redes 5G. El despliegue de la tecnología 5G es uno de los diez ejes principales de la Agenda España Digital 2025 que pretende desarrollar el Gobierno, por lo que no solo supondrá un cambio tecnológico en las redes de comunicaciones móviles, sino que también tendrá un impacto en el conjunto de la economía y la sociedad.

Pronto verá la luz la nueva Ley de Ciberseguridad 5G, ¿con qué objetivo se elabora esta Ley?

Esta Ley se crea con el objetivo de establecer un marco confiable y seguro que incentive el despliegue y la inversión por parte de los operadores de telecomunicaciones y la demanda de los servicios por parte de los usuarios a fin de impulsar el desarrollo de la tecnología 5G en España.

Las redes 5G poseen ventajas comparativas en seguridad respecto a las de generaciones precedentes, sin embargo, también presentan nuevos riesgos debido a su compleja red de arquitec-

tura, ¿a qué tipo de riesgos en ciberseguridad nos enfrentaremos?

Los riesgos a los que nos enfrentamos son los mismos que en tecnologías anteriores. Sin embargo, en el 5G se ha tenido en cuenta la seguridad desde el diseño, desde las especificaciones técnicas, si bien es cierto que se trata de una red más compleja que las anteriores, incluyendo elementos de la virtualización dentro de la infraestructura.

¿En qué medida puede afectar esta Ley a operadores y suministradores de servicios 5G?

Es importante que esta Ley fije de forma expresa los criterios a tener en cuenta de los operadores de telecomunicaciones en el esquema de seguridad y en la estrategia de diversificación por parte de los operadores. Se van a realizar fuertes inversiones en redes 5G por parte de los operadores y es necesario partir de un marco de certidumbre para acometer estas fuertes inversiones.

¿Qué tipo de medidas técnicas y de organización deberán adoptar los operadores y suministradores de servicios 5G?

El anteproyecto de Ley establece que los operadores de telecomunicaciones tienen que realizar el análisis de riesgos de los suministradores y adoptar las medidas para mitigar los riesgos. Sin embargo, consideramos relevante que sean los propios suministradores quienes realicen sus propios análisis de riesgos y sus propias medidas de mitigación. Nadie mejor que ellos pueden solventar cualquier problemática que pueda surgir en relación a los riesgos de los propios suministradores.

En mi opinión habría que tener más certidumbre en la Ley a la hora de obligar a un operador a prescindir total o parcialmente de un suministrador que la administración califique de alto riesgo. Como hemos comentado, los operadores van a realizar fuertes inversiones y necesitan certidumbre a la hora de invertir. Por tanto, consideramos que por ejemplo la Administración debería certificar a determinados suministradores, de forma que sean calificados como aptos y, en el supuesto de que en un futuro considere que el operador deba prescindir de dicho suministrador, sea compensado por la propia administración. El dejar abierto la posibilidad de que la Administración pueda obligar a un operador a prescindir total o parcialmente de él no genera la certidumbre que los operadores requieren para acometer las inversiones necesarias para el despliegue de redes 5G.

Según el Anteproyecto de Ley de Ciberseguridad 5G, las sanciones por la comisión de infracciones muy graves llevan aparejada una multa de hasta 20.000.000€. ¿Cuál puede ser el impacto de un incidente de seguridad "muy grave" en las redes 5G?

En este punto hay que diferenciar la sanción con el incumplimiento de la ley de sufrir un incidente de seguridad. Son dos cosas muy diferentes, que tengas un incidente no significa directamente

que debas tener una sanción.

El régimen sancionador está basado en la Ley de telecomunicaciones, que tiene su propio régimen, ya vigente, que se amplía con las infracciones:

- El incumplimiento de las obligaciones establecidas en el Esquema de seguridad para las redes y servicios 5G cuando sean directamente exigibles, lo que constituirá una infracción grave.

- El incumplimiento de las resoluciones dictadas por órganos competentes, lo que constituirá una infracción grave.

El borrador del anteproyecto define: "Constituirá una infracción grave cuando el requerimiento se dirija a los operadores o a los suministradores y haya pasado un mes desde la finalización del plazo para su cumplimiento."

¿Qué criterios pretende el Gobierno seguir para analizar las vulnerabilidades ligadas a la cadena de suministro?

Estos criterios no están fijados en el Anteproyecto. Se remiten a un Real Decreto posterior. Consideramos que estos criterios deben fijarse en el Anteproyecto que ha sido sometido a consulta.

La Comisión Europea u organismos como el European Data Protection Board o la Agencia Española de Protección de Datos, siempre han animado a las empresas a contar con certificaciones oficiales en ciberseguridad, sin embargo, no son obligatorias ¿establece la nueva Ley de Ciberseguridad 5G esta condición de obligatoriedad?

El Anteproyecto no fija esta condición y, sin embargo, consideramos que deben establecerse o bien de forma obligatoria o bien de forma voluntaria, pero además debe fijarse que si el operador de telecomunicaciones utiliza un suministrador que ha sido certificado por parte de la Administración, en el caso de ser considerada como de alto riesgo y obligar al operador a prescindir del suministrador, la Administración debe compensar al operador por las inversiones efectuadas.

¿Cuál ha sido la respuesta por parte del sector de las telecomunicaciones? ¿Cree que están preparados?

Los operadores siguen reclamando mayor certidumbre a la hora de invertir en redes 5G de forma que dichas inversiones no sean infructuosas.

¿Qué proceso de adaptación se llevará a cabo para implantar la legislación?

Con las obligaciones fijadas en el Anteproyecto de Ley, como mínimo, los operadores requieren de 12 meses para adaptarse a la Ley. El anteproyecto establece que en el plazo de 4 meses los operadores deberán presentar un análisis de riesgos sobre las redes desplegadas o que se vayan a desplegar en los próximos dos años, pero este plazo es de imposible cumplimiento por parte de un operador de telecomunicaciones.

FIRMA INVITADA

El arancel digital oculto de la ciberseguridad en la transformación digital

Daniel Largacha

Es obvio decir que la digitalización ha llegado a nuestras vidas, no es que esta llegada se materialice ahora, lleva tiempo macerándose, pero ha sido en estos tiempos extraños en los que todos los actores (ciudadanos, empresas y gobiernos) han tenido que recurrir a esta para poder mantener el modelo de sociedad que hemos construido de la mejor manera posible.

Las empresas de tecnología pueden estar satisfechas (y lo están), ni mucho menos ellas tienen responsabilidad alguna con la situación actual, dado que la digitalización era una tendencia consolidada que se estaba instaurando. No obstante, no por ello es menos cierto que se ha acelerado unido forzosamente al aumento del grado de aceptación (y adaptación) que hemos realizado todos los actores.

Algunos datos que refuerzan esta tendencia los podemos encontrar en algunos estudios o hechos como los siguientes:

- Incremento de la digitalización de los consumidores: se ha producido incremento del 25% en el uso de dispositivos móviles

(smartphones y tablets) en la era pos-pandemia.

- La adhesión de negocios a los canales digitales: como por ejemplo el incremento del 60% en el alta de establecimientos de comida en plataformas digitales.

- Uso mayoritario del teletrabajo: el aumento del teletrabajo del 15% en la época pre COVID al 25% en la actualidad, cifra de cobertura que sería mayor si pudiéramos tener en cuenta el porcentaje de trabajos que no admiten la modalidad de teletrabajo por el tipo de prestación.

- Mayor adopción de tecnologías Cloud: el incremento del uso de tecnologías en la Cloud en 2020 con un 82% de las empresas acelerando el uso de estas tecnologías con el fin de agilizar y disponibilizar las tecnologías para empleados, proveedores y clientes.

La digitalización ha llegado para quedarse, y seguramente asistiremos en los próximos años a un aceleramiento, no obstante este nuevo escenario ofrece nuevas posibilidades para otros inesperados actores.

Escenario actual

A nadie se le escapa que hoy en día tanto las empresas como los gobiernos basan su modelo operativo en las tecnologías de la información, no es una cuestión en la que tengamos que estar de acuerdo, simplemente es la realidad. Esta adopción de la tecnología lleva asociada una serie de riesgos inherentes que han estado ocultos a los ojos de muchos durante mucho tiempo. Estos ciber riesgos existen y han existido siempre, pero es ahora cuando toman una especial relevancia.

Es injusto señalar a un sector de los actores por falta de adaptación (empresas y gobiernos), la situación actual responde a la ausencia de una verdadera cultura de seguridad en todos los ámbitos que se ha ido cocinando a fuego lento desde hace varias décadas.

Según datos de la Interpol de agosto de 2020, el número de ataques por ransomware había crecido en un 36% con respecto a todo el 2019. Este preocupante panorama no responde únicamente al oportunismo de cibercriminales, responde a esta situación que señalaba una situación que se ha ido cocinando durante décadas. Y según los pocos datos agregados que se dispone, a la vista del retorno que ofrece el ransomware, veremos un aumento sustancial en los próximos meses (según unas consultoras que han realizado seguimientos de algunos de los monederos empelados por Ryuk, los ingresos ascienden a 150 millones de dólares).

A día de hoy, los ataques por Ransomware junto con el tipo de ataques BEC (o mal llamado "Fraude al CEO") copan el 80% de las pérdidas producidas a organizaciones. Si miramos a los datos con perspectiva anual, no parece que la situación vaya a cambiar, por muchos esfuerzos que hagan los gobiernos mediante prohibiciones de escaso efecto.

DANIEL LARGACHA

Cyber Security Centre Director, ISMS Forum;
Global Control Center CERT Assitant Director, Mapfre

Es cierto que esa cultura de seguridad está cambiando, al menos en algunas capas del ecosistema empresarial. Las empresas de software cada día adquieren mayor responsabilidad de la importancia de poner en el mercado productos que sean seguros, y que además tengan su aproximación continua en el tiempo que todo producto de seguridad requiere.

De los dos mayores problemas a los que se enfrenta una organización, BEC y ransomware, es este segundo el que realmente plantea un riesgo material de suficiente relevancia para que las empresas lo tomen con la importancia que le merece. No es una tarea sencilla, dado que las bandas que están detrás de este ransomware tienen algunas peculiaridades que lo diferencian de otro tipo de ciber riesgos:

- Profesionales altamente cualificados y con recursos suficientes (exploits, zero days, ...etc) y con capacidad.
- Están entrenados y formados para ejecutar las tareas con determinación.
- Tienen recursos humanos suficientes para poder hacer frente al menos en número a un departamento de seguridad.

Las organizaciones están tomando consciencia de lo relevante de este asunto, posiblemente un ataque por ransomware hoy en día puede ser el evento más probable y que puede amenazar en mayor grado la viabilidad de una organización,

por grande que esta sea.

Dentro de esta consciencia que están tomando las organizaciones, y de las líneas de actividad que están poniendo en marcha (más allá de las habituales) hay una serie de actividades que tienen una mayor relevancia, por su efecto mitigador en el caso de ataques de tipo Ransomware:

- Aproximación a Zero Trust: un único equipo que esté ubicado en la red interna y que se encuentre bajo el control de un cibercriminal es el punto necesario para poder empezar la cadena de ataque.

- Mejorar la visibilidad de los endpoints: las tecnologías EDR son un must a día de hoy, tan importantes y básicos como un Antivirus. No son la panacea pero aportan un nivel de visibilidad en endpoints necesario para la detección temprana de este tipo de ataques.

- Mejora de las capacidades de monitorización: la aproximación a la monitorización debe ser más intensa. El enemigo está fuera de la red interna, pero hay que contar con que ya puede estar en la red interna. El mismo foco que se ponga en los ataques de fuera hay que ponerlo en los ataques o movimientos que se puedan realizar desde la red de interna.

- Mejorar el control de usuarios privilegiados: última piedra angular de los ataques por ransonware, el objetivo de los ciber criminales desde los que finalmente suelen lanzar la ejecución del ransomware y con los que consiguen ganar resistencia.

- Reducir los tiempos de respuesta más allá de enfocarlos en procedimientos, hay que ganar en agilidad de forma efectiva. Las herramientas de tipo XOAR aportan un conjunto de ventajas interesantes que permiten prescindir de la intervención humana, o al menos reducirlo a lo realmente necesario, permitiendo enfocar los (escasos) profesionales expertos en esta área.

Que podemos esperar del futuro

Sería fantástico que la implantación de las medidas de seguridad comentadas fuera suficiente para atajar la situación, aunque detrás de estas se requiere profesionales expertos en tecnologías que escasean. Pero desafortunadamente no es así.

Es difícil aventurar lo que nos depara el futuro, pero con una lectura muy simple podremos identificar dos tipos de organizaciones:

- Aquellas que son realistas con la gravedad del escenario y han desplegado tanto las medidas de seguridad descritas anteriormente como el resto de medidas razonables de las que que ya debe disponer una organización diligente.
  Aquellas que por cualquier causa no sean capaces de desplegar estas medidas.

Lo más probable es que los ciber criminales se enfoquen en este último grupo de organizaciones, dado que lo que buscan es un retorno económico rápido y que les conlleve el menor esfuerzo y uso de recursos (que a ellos también les cuestan). Ahora bien ¿esto significa que las primeras estarán libres de ataques?

Ojalá el futuro nos muestre que nos hemos equivocado, pero probablemente no. Es razonable pensar que en paralelo a la tendencia anteriormente mostrada, es probable que también empecemos a ver ataques que muestren los siguientes comportamientos:

- Ataques relámpago: a día de hoy los ciber delincuentes suelen emplear varios días en las redes de su víctima hasta que consiguen disponer de todo lo necesario para hacer un ataque de alcance completo.

- Uso de software común: denominado LOL, que se basa en el uso de un software que suele disponer de caja los sistemas y que es más que suficiente para llevar a cabo las actividades que requieren. El uso de este tipo de herramientas reduce significativamente las posibilidades de detección por parte de la víctima.

- Uso de esteganografía: la descarga de artefactos o binarios suele ser necesario para poder ejecutar algunos exploits específicos o para poder ganar persistencia. El control de ficheros tipo EXE o el control del tráfico descargado está al orden del día en muchas organizaciones. No obstante, la esteganografía permite a un atacante poder descargar o exfiltrar información de forma prácticamente desapercibida que escapa a la monitorización de los EDR.

- Empleo de usuarios menos privilegiados: la búsqueda de usuarios especialmente privilegiados es una tarea que empieza a ser detectada en las organizaciones. Sin embargo, para poder llevar a cabo un ataque de ransomware no es necesario hacerse con el control de un usuario de tales características, es suficiente con un usuario que tenga privilegios para poder controlar parte del parque de los servidores o de las workstations de una organización.

Las organizaciones van a tener que ser especialmente rápidas en la adopción de las medidas de seguridad que se han descrito en el punto anterior. Aquellas que sean exitosas podrán centrarse en poner medidas de control para atajar los ataques que aún están por descubrir.

Este contexto viene a estresar aún más si cabe el complicado escenario de inversión que deben acometer las organizaciones, pero que sin duda deben de tener en cuenta aquellas que tengan intención de mantenerse en un mundo digital, ¿o es que tenemos alguna otra opción?.

Tú tienes poder sobre tu mente, no sobre los acontecimientos. Date cuenta de esto, y encontrarás la fuerza.
Emperador Marco Aurelio, II a.c.

PROYECTOS DE INTERÉS

Conoce a los ganadores de la II Edición de Emprendimiento e Innovación de ISMS Forum

ISMS Forum presenta las cuatro tecnologías innovadoras en ciberseguridad ganadoras de la *Segunda Edición de Emprendimiento e Innovación de ISMS Forum*, una iniciativa que trata de dar visibilidad e identificar nuevas soluciones y tecnologías de ciberseguridad en el ámbito del Gobierno de la Ciberseguridad. De entre todas las propuestas recibidas, han destacado: Countercraft, Epic Bounties, Ironchip y VMRay.

CounterCraft

La Cyber Deception (que podría traducirse como "ciberengaño") es una tecnología de ciberseguridad innovadora que cada vez está cobrando más fuerza. Permite la detección de amenazas en sus fases iniciales, generando inteligencia personalizada y de gran calidad sobre las mismas. Asimismo, proporciona defensa activa, incrementando los costes para los ciberatacantes y disminuyendo los de las organizaciones.

La Cyber Deception complementa otras tecnologías de ciberseguridad sin causar interrupciones en su actividad, o se incorpora en ausencia de las mismas para detectar con poco coste escenarios actualmente complejos como de detección en entornos SCADAS, SWIFT, redes WiFi o redes OT (tecnología de operaciones), entre otros.

epicbounties

La plataforma ofrece un servicio de detección de vulnerabilidades que no existe actualmente en los proveedores de la industria española.

Este modelo facilita que las empresas cuenten con programas contínuos de detección de vulnerabilidades llevados a cabo por una comunidad de élite de investigadores en la materia.

Solo consumirá presupuesto al sumar nuevas vulnerabilidades identificadas. Ideal para entornos con un nivel de seguridad alto con un coste de localización de vulnerabilidades de larga duración.

Al regular el número de investigadores participantes, se puede acelerar al máximo la búsqueda de nuevas vulnerabilidades.

Su tecnología crea y certifica una identidad utilizando un dispositivo y una ubicación sin GPS. Se consigue mediante el análisis de las ondas de radio (wifi, 2g,3g,4g,5g...) de ese lugar, creando una firma única. Esto permite asociar de forma segura la identidad del usuario a esa ubicación, reemplazando o fortaleciendo las contraseñas de una manera completamente diferente a la disponible en el mercado.

A través de esta solución, se integra una capa de seguridad adicional para la mayoría de los sistemas y procesos informáticos, asegurando así que el trabajador solo pueda conectarse a su lugar de trabajo desde el sitio establecido, deshabilitando las operaciones fuera de estos lugares.

Por otro lado, protege y controla la seguridad a lo largo de la cadena de valor de las infraestructuras críticas, determinando y controlando qué empleado o proveedor puede acceder a estas instalaciones.

La plataforma se basa en la innovadora tecnología sandbox, que supera los defectos inherentes a las soluciones de sandbox basadas en el enlace y la emulación del sistema.

Sandboxing es la tecnología que permite detectar y analizar comportamientos maliciosos y dar el veredicto final y completo. Pero sandbox regular tiene varios problemas. En primer lugar el malware detecta la existencia de la sandbox y lo silencia.

La propuesta de VMRAY consiste en proporcionar a los equipos SOC y CSIRT una Sandbox no detectable por malware, con el análisis de comportamiento avanzado y la detección máxima de los ataques híbridos.

Su enfoque reside en la inspección multicapa, un análisis totalmente automatizado e interactivo, la detección de phishing, la extracción automatizada de los IOCs, las imágenes doradas, y localización en la nube.

Un año más, ISMS Forum trabaja con el objetivo de visibilizar nuevas soluciones del sector de la ciberseguridad orientadas a proporcionar a las empresas la máxima protección y capacidad de respuesta frente a un escenario donde cada vez hay más sofisticación en el ataque.

Desde ISMS Forum agradecemos la amplia participación y animamos a aquellos interesados a enviar sus propuestas de cara a la Tercera Edición de Emprendimiento e Innovación de ISMS Forum.

El Observatorio de Ciberseguridad de ISMS Forum Barcelona lanza el Indicador de Madurez en Ciberseguridad

El objetivo del Indicador de Madurez en Ciberseguridad es analizar el nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información, así como generar indicadores nacionales sobre el estado de la ciberseguridad en empresas y entidades privadas y públicas.

El Indicador de Madurez en Ciberseguridad se presenta como un divulgador de conocimiento e investigación a través de la creación de métricas y referencias nacionales, y la interlocución con instituciones y reguladores.

El estudio ha revelado que más del 60% de las empresas cuentan con una política donde se definen los roles y responsabilidades, junto con los requerimientos legales y regulatorios, dentro del marco de los procesos de gobierno y gestión del riesgo de ciberseguridad. Asimismo, cerca del 50% de las empresas identifican y comunican las dependencias y los requisitos de los servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización. Sin embargo, el inventario de dispositivos, sistemas, aplicaciones y recursos de información solo es completo en un tercio de la muestra. El documento recoge que hasta un 50% de las empresas mantienen identificadas y documentadas las vulnerabilidades y amenazas de ciberseguridad, pero solo el 30% de la muestra manifiesta que los procesos de gestión del riesgo, así como el nivel de tolerancia, están establecidos, acordados e informados con las partes interesadas.

En cuanto a la protección de los sistemas y activos de información, más del 40% de las empresas manifiesta documentar los procesos y procedimientos, y más del 50% identifican los datos, pero los protegen de manera parcial. Casi la mitad de las empresas encuestadas manifiesta la existencia de una gestión de identidades y accesos en base al principio de menor privilegio y segregación de funciones, sin embargo, en la gestión del cambio, si bien la mitad de los encuestados afirma la realización de un mantenimiento de los sistemas de información de forma controlada, los accesos no se auditan.

Consulta la Guía para la gestión de crisis por ciberincidente en la cadena de suministro

El ISMS Forum -International Information Security Community-, junto al Data Privacy Institute, publicó la *Guía práctica para la gestión de riesgos de terceros en privacidad*, en el marco de la XXII Jornada Internacional de Seguridad de la Información el pasado 26 de noviembre de 2020.

Cada vez resulta mayor la dependencia de las empresas de sus proveedores y de la cadena de suministro, el deber de diligencia de las empresas no solo va a suponer un mayor conocimiento de la cadena de suministro y una mejora en la toma de decisiones, sino que además esa diligencia debida constituye una obligación legal impuesta por la normativa de protección de datos pero también otro tipo de normativas, como por ejemplo la penal, o normativas sectoriales específicas.

El objeto de la misma es establecer unas pautas generales, recomendaciones o buenas prácticas que permitan a las empresas concretar e implementar el principio general de la diligencia debida, especialmente a la hora de elegir a sus proveedores. Tras definir las obligaciones legales existentes, el documento aborda cuáles son las buenas prácticas según la fase en la que vaya teniendo intervención el proveedor: fase precontractual, fase contractual y fase de terminación de la relación contractual.


Aiuken
Cybersecurity

Akamai

aruba
a Hewlett Packard
Enterprise company

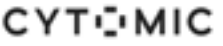
BeyondTrust

BITSIGHT

Check Point
SOFTWARE TECHNOLOGIES LTD.

cipher
a PROSEGUR company

CLOUDFLARE

CROWDSTRIKE

CYTOMIC

DARKTRACE

Deloitte.

fastly

FIREEYE

Forcepoint

FORESCOUT

ForgeRock

FORTINET

SIA
An Indra company

HUAWEI

IBM

McAfee

netskope

NEXTVISION
SecurityScorecard

GLOBAL


okta

OneTrust

paloalto

PCYSYS

proofpoint.

Pulse Secure

Qualys.

radware

Recorded Future

retarus
global messaging

riskrecon

S21
SEC

SAMSUNG

SentinelOne

SOPHOS

thycotic

transmit
SECURITY

TREND
MICRO

VARONIS

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