isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

CSC CYBER SECURITY CENTRE

GOBIERNO DE LA CIBERSEGURIDAD:

RETOS Y OPORTUNIDADES

XI FORO DE LA CIBERSEGURIDAD

ORGANIZADO POR EL CYBER SECURITY CENTRE (CSC) DE ISMS FORUM

MAYO 2022

PROTAGONISTA
Don Gibson (UK Gov)
Tecnología bien diseñada y entregada

FIRMAS INVITADAS
Guillém Colóm, Pedro López y Carlos A. Saiz

CISO ROUND TABLE
Los retos del buen gobierno de la ciberseguridad

www.ismsforum.es

DANIEL LARGACHA LAMELA

Director del Cyber Security Centre de ISMS Forum

ISMS FORUM

ismsforum.es

La digitalización del arte de la guerra

CAPACIDADES CIBER EN UN CONTEXTO BÉLICO

Desde finales del siglo XX, la digitalización ha cambiado la forma en la que se desarrolla el comercio y ha contribuido a crear un mundo más conectado e interdependiente a todos los niveles: estados, empresas e individuos. Es un aspecto que ya se puso de manifiesto durante la pandemia y en las diferentes crisis que han afectada a la demanda de determinados productos a nivel mundial.

La digitalización era algo que podíamos observar en ámbitos comerciales y sociales, pero, para la sociedad en general. no era algo tan evidente su uso en otros escenarios como puede ser un enfrentamiento bélico real.

> **Todo hace pensar que Rusia se está guardando todas estas tecnologías para episodios futuros**

ATAQUES CIBERNÉTICOS

Como si se tratase de un metaverso, de una realidad paralela, durante los últimos tres meses se ha bombardeado a la sociedad con contenidos que explican el modo en el que países como Rusia utilizan técnicas cibernéticas para atacar a sus enemigos. Es más, tres horas antes de que el primer proyectil impactara en tierra ucraniana, o de que cualquier soldado soviético pisara terreno hostil, Rusia lanzó el primer ataque en el ámbito cibernético frente a las principales instituciones gubernamentales y empresas críticas de Ucrania, en un intento por generar confusión y debilitar al enemigo.

No es la primera vez que todas estas capacidades cibernéticas han sido utilizadas en conflictos bélicos, pero sí es la primera vez en la que se han expuesto con tan amplio detalle para el análisis de los profesionales. Es cierto que, gracias a toda esta información hemos podido ver que no se han utilizado *zero days* o técnicas y herramientas avanzadas que podrían haber mostrado el enorme potencial que Rusia tiene en el desarrollo de estas capacidades cibernéticas.

DOCTRINA GERASIMOV

A los profesionales que nos dedicamos a la ciberseguridad, este escenario nos hace pensar que resulta más que probable que Rusia se esté guardando todas estas tecnologías para episodios futuros, teniendo en cuenta que son de un uso limitado tras su publicación. Esto les permitiría ejercer su poder en este ámbito y sacar partido de la debilidad de los contrincantes, utilizando estas habilidades como medida coercitiva, antes de tener que hacer uso de capacidades de mayor calado, como pueden ser las nucleares.

La postura de Rusia no es nueva, y no sorprende a los analistas militares. Básicamente se le está dando continuidad a la Doctrina Gerasimov, que lleva el

nombre de un general ruso. A grandes rasgos, establece que, en algunos ámbitos y de cara a la consecución de un objetivo concreto, las capacidades cibernéticas podrían exceder con creces las que pudieran obtenerse a partir de armas convencionales. Esta doctrina, que tiene ya algunos años, permite anticipar el modo en el que Rusia pretendía potenciar las capacidades ciber con fines militares.

» EL *HACKEO* A SOLARWINDS

Teniendo en cuenta todo esto surge una cuestión que va más allá de las razones por las que Rusia no ha utilizado sus capacidades ciber. Lo realmente importante es saber si este país ya las ha desplegado y tan sólo está esperando el momento adecuado para sacar el mayor beneficio de ellas.

No hay que olvidar que hace poco más de un año se descubrió la mayor intrusión realizada —supuestamente— por un estado: el *hackeo* a Solarwinds, del que no se han conocido todavía muchos detalles acerca de su impacto. ¿Y si el *hackeo* fue un intento de Rusia de tener su propio "botón de desactivación operativo" frente a sus enemigos? ¿Y si, a día de hoy, ya ha conseguido su objetivo, pero lo tiene un eterno letargo?

Por encima de todo, lo que se puede afirmar es que la digitalización desgraciadamente ha llegado al ámbito bélico y se ha normalizado su uso. Incluso, todo hace indicar que se está utilizando de manera generalizada frente a estados a los que no se les ha declarado la guerra, pero sobre los que se quiere ejercer una influencia o presión, o simplemente ocasionar una merma en sus capacidades. «

DIRECTOR GENERAL
Daniel García

SUBDIRECTORA
Beatriz Díaz

CONSEJO EDITORIAL/ REDACCIÓN
Cynthia Rica
María Manjón

EQUIPO DE GESTIÓN
Beatriz Lozano
Beatriz García
Cynthia Rica
Leire Ruiz
María Manjón
Virginia Terrasa
Wasim Escribano

HAN COLABORADO
Daniel Largacha
Alberto López
Esther Muñoz
Jesús Mérida
Javier Lomas
Guillém Colóm
Pedro López
Carlos A. Sáiz

PÁGINA WEB
www.ismsforum.es

Curso de Gestión de riesgo IT en Supply Chain

FORMACIÓN

Este curso de 30 horas y media tiene como objetivo principal ofrecer una visión holística desde un punto de vista estratégico para una gestión segura de una cadena de suministro, así como de los riesgos tecnológicos que pueden materializarse sobre ésta. Los fundamentos teóricos se complementarán y consolidarán mediante su adaptación a entornos reales y la realización de casos prácticos.

CONTENIDO

Introducción a la cadena de suministro (supply chain)
Gestión del riesgo IT en el ciclo de vida del proveedor
Gobierno de ciberseguridad en supply chain
Análisis y gestión del riesgo IT en supply chain
Gobierno IT en supply chain
Monitorización del riesgo IT en supply chain
Auditoría IT de proveedores
Privacidad y cumplimiento contractual en supply chain
Innovación y Transformación en supply chain
Estándares y herramientas
Integración de IT en supply chain

¿A QUIÉN VA DIRIGIDO?

Este curso está dirigido a aquellos profesionales, independientemente de si poseen un perfil tecnológico, de gestión o legal, que deseen adquirir una visión transversal de los riesgos tecnológicos presentes en una cadena de suministro y las estrategias para gestionarlos.

PRÓXIMA EDICIÓN

La siguiente convocatoria se realizará en SEPTIEMBRE de 2022 en modalidad online.

Fechas: del 14 al 29 de septiembre de 2022. El curso se divide en 10 sesiones.

Horario: El horario de conexión en remoto será de 16:00 a 19:00 (3 horas diarias).

INFÓRMATE

Escríbenos a formacion@ismsforum.es
www.ismsforum.es
(+34) 915 63 50 62

Una iniciativa de

isms FORUM | INTERNATIONAL INFORMATION SECURITY COMMUNITY

La ciberseguridad es la manifestación de una tecnología bien diseñada y entregada

Don Gibson.

DON GIBSON,
Head Of Cybersecurity, Dept. For International Trade (DIT), UK Gov.

Pasó directamente de la universidad al área de tecnología de los bancos de inversión y, de ahí, al área de seguridad de la información y el riesgo en diferentes entidades relacionadas el sector del juego, el financiero, el farmacéutico, viviendo en primera persona experiencias —como el ataque de ransomware global— que le impactaron especialmente. En la actualidad es el responsable de Ciberseguridad en el departamento de Comercio Internacional del Gobierno de Reino Unido.

¿Cómo contribuye la ciberseguridad en la transformación de las organizaciones?

Bueno, en primer lugar, la ciberseguridad está ahí para potenciar el negocio y a las personas, y tiene que hacerlo bien. En esencia, en realidad es la manifestación de una plataforma tecnológica bien diseñada y entregada. Como tal, hay que asegurarse de que es apta para el propósito para el que fue diseñada, de que hay patrones de diseño repetibles y de que hay puntos de referencia circulares para que todo funciona como se supone que debe hacerlo. Lo mejor es poder comenzar a trabajar desde el principio, junto con los procesos a establecer. De hecho, cuando se empieza a hablar de todo esto, una de las primeras cosas que hay que establecer es la seguridad. Antes de comenzar a trabajar en cosas reales hay que entender y averiguar realmente lo que vamos a hacer.

¿Las compañías están al día en ciberseguridad?

Las empresas occidentales sí están en una buena posición respecto a este tema o, al menos, en una posición mucho mejor que la que tenían hace unos años.

En los consejos de administración les gusta contar con personas personas inteligentes, y la gente inteligente aprende de los errores de los demás. Por lo tanto, si ves que se están atancando sitios con *ransomware* a derecha e izquierda, sabes que el peligro está ahí fuera. No es una amenaza inventada.

Aunque es verdad que las empresas están en un buen punto, sí es cierto que no todas cuentan con los mismos mecanismos o con la forma correcta de control de amenazas.

¿Qué importancia se atribuye a la ciberseguridad?

Solo puedo hablar por mí como profesional. No puedo hablar en nombre del Gobierno de Reino Unido. En cualquier caso, la ciberseguridad es la prioridad número uno en todos los ámbitos.

Cuando algo va mal, se culpa a la ciberseguridad. Si alguien se cuela porque no se ha parcheado algo correctamente... Ohh, ese un problema de ciberseguridad. Pero ¿por qué es un problema de ciberseguridad? ¿Porque no se hizo bien el trabajo? ¿Porque no se sabía que eso estaba ahí? ¿Por qué la gente no se da cuenta de que esto es un "problema de todos"? Cuando algo va mal es un problema de negocio: de RRHH, de comunicaciones, de legal, de comercial... y de ciberseguridad, de tecnología, de la junta directiva... Es un problema de todos.

Por lo tanto, todo el mundo tiene que hacer algo al respecto. La ciberseguridad está ayudando a transformar el mundo en cuanto a la capacidad de procesamiento que tienen las personas. Contemplemos la banca móvil, por ejemplo. Hace cinco años dije que la mayoría de las personas realizarían operaciones bancarias en sus teléfonos y lo harían de forma segura y entendiendo qué es biometría, qué es MFA (autenticación de múltiples factores) ... Y aquí estamos ahora. La banca *online* está ahí y todo se entrega de forma segura. Eso es gracias a la ciberseguridad.

¿Hay paralelismos entre el crecimiento de estos servicios digitales y la ciberseguridad?

Sí. Por ejemplo, en el Reino Unido tenemos el rastreador COVID para ver si has estado en contacto con alguien positivo. Hace poco viajé a España y pude entrar sin problema por que me escanearon allí mismo la prueba de vacunación. Sin embargo, lo que realmente no me gusta acerca de este sistema es que todo el mundo se utilice códigos QR. No me gusta el hecho de tener que dejar que mi navegador apunte a donde indieque estos QR, o que mi cámara abra el navegador o cualquier otra cosa.

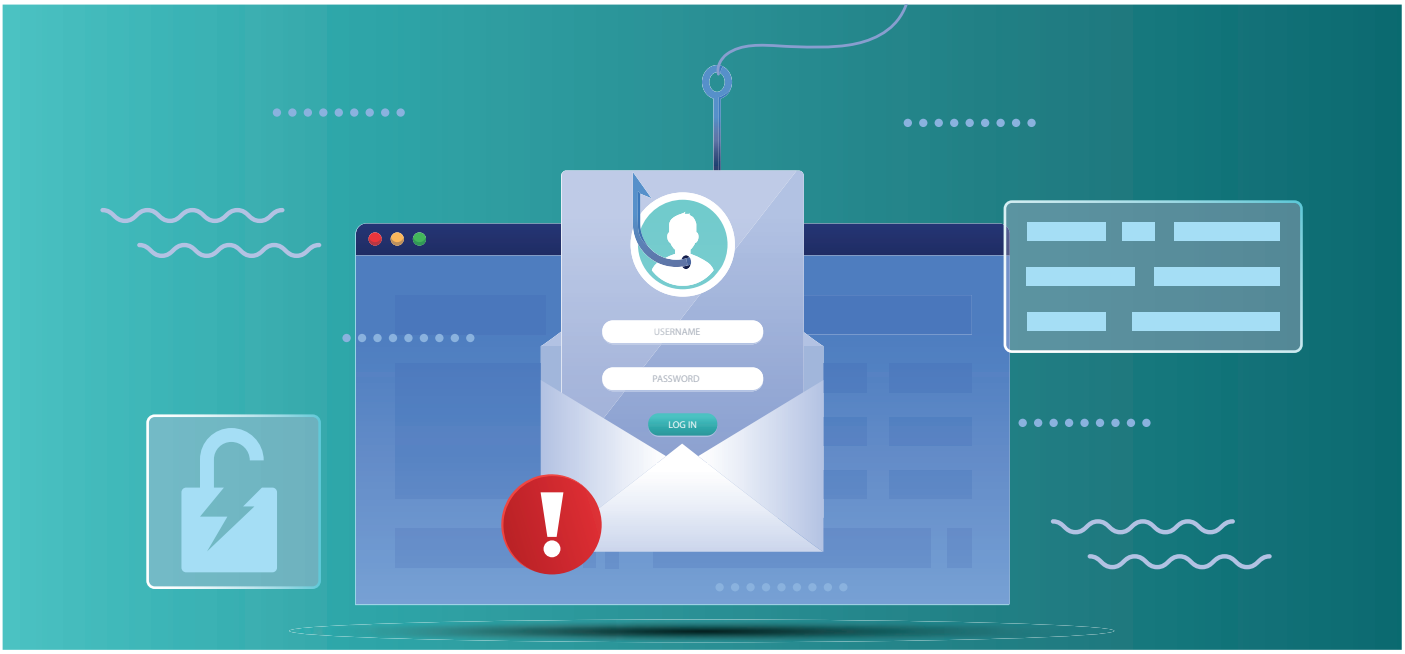
En la actualidad estamos viendo el *phishing* también en códigos QR. Han acuñado ya el término "*quishing*" para referirse a ello. En cambio, si puedes conseguir que todo eso se ejecute en un *sandbox* (un entorno seguro), estaría mucho mejor. O, por ejemplo, si solo puede abrir una única página web que no pueda llamar a nada más sin que haya una interacción física del usuario. Algo así, estaría mucho mejor y sería más seguro.

De hecho, todo esto se puede resumir en dos palabras: seguridad y tranquilidad. En primer lugar, es necesario comprobar que todo está bien y funciona correctamente. Esto es lo que proporciona la "seguridad", y es lo que da la "tranquilidad" de que los datos no están en riesgo, que nosotros no estamos en riesgo, que la empresa no está en riesgo. Las personas esperan seguridad tanto en casa como en la oficina, y la ciberseguridad puede ofrecérsela.

> **"Estamos viendo el phishing también en códigos QR. Se ha acuñado ya el término "quishing" para referirse a ello**

¿Cuáles son las claves para aplicar y gobernar la ciberseguridad?

En primer lugar, tenemos que entender por qué estamos haciendo algo. Si es para cumplir con una nueva ley que se avecina, hay que tener muy claro qué es lo que se necesita. También puede tratarse de una exigencia empresarial, de algo que la empresa ha decidido que tiene que mejorar. Un ejemplo: muchos cajeros automáticos siguen utilizando Windows NT y necesitan ser actualizados a un sistema operativo mucho más seguro, generalmente será Windows 10. Pero ¿cómo se consigue ese cambio? ¿Cómo



El vector más sencillo de atacar es el de la tecnología porque siempre está encendido, necesita parches, atención...

se garantiza el funcionamiento de los sistemas? Por último, puede tratarse de un proyecto de vanidad: bien que la junta directiva quiera algo brillante para enseñar —y decir: "¡Hemos hecho esto!"— o bien se trata del último hurrá de un CTO o un CIO que quiere hacer algo para dejar su legado. Los últimos dos son los que dan miedo.

Lo primero es saber **por qué** necesitas la seguridad y, después, asegurarse de que tienes una muy buena relación con el departamento de gestión de proyectos y con los jefes de proyecto que están a tu cargo. Para ello, es importante hacer un esfuerzo adicional, crear elementos y ayudas para ellos sin que te lo pidan. Hay que darles una línea base de requisitos muy simple. Esto ayuda a construir lo que yo llamo "capital social".

Cuando ya tienes ese capital social y la confianza del equipo —y este se da cuenta de que estás trabajando con ellos para ayudar a entregar sus proyectos tan rápido como sea posible, tan seguros como sea posible—, entonces puedes empezar a plantear cualquier otra cosa que venga y que no se haya anticipado.

También necesitas trabajar de forma muy estrecha con el departamento legal y comercial. Hay que mostrarles cariño. Básicamente, tienden a ser, digamos, "odiados" en los proyectos porque son bloqueadores, van lentos, los contratos tardan mucho en aprobarse o cualquier otra cosa por el estilo. Así que cualquier cosa que puedas hacer para facilitarles la vida, en el sentido de la ciberseguridad, será realmente útil.

Por último, empleo mucho la palabra "trueque". Normalmente trabajo en el departamento de desarrollo y, digamos, que un desarrollador ha descubierto cómo utilizar un estándar biométrico y ha creado una buena biblioteca. Y resulta que otro equipo está empezando a enfrentarse a ese mismo problema, así que lo que hago es facilitar el contacto entre ambos. De este modo, el segundo equipo acaba de ahorrarse un *sprint* de dos semanas y ahora puede dedicar su tiempo a buscar la seguridad que necesitan.

Esas son las claves principales. Se necesita mucho trabajo de campo para hacerlo, pero cuando la gente realmente lo entiende y lo comprende, entonces es cuando se ven los beneficios.

¿Qué ocurre cuando ese capital social cambia?

Depende de lo que haya motivado el proyecto. Si se trata de un asunto de *compliance*, entonces no importa lo que quiera o piensen las personas que se incorporan. La motivación es que lo hacen por una razón legal. Pero en los proyectos "vanidad" que he mencionado antes, es cuando hay que tener cuidado.

En cualquier caso, lo bueno de cualquier trabajo que hayas hecho es que siempre se puede reutilizar en el futuro. Así que, si has construido elementos, librerías o diagramas de flujo de datos, y tienes los sistemas funcionando y las metas han sido acordadas entre todos... pues puede ser reutilizado. El truco está en estar implicado en el proyecto.

Sin embargo, si alguien muy arriba cambia de opinión y dice "ya no vamos a hacer esto, sino otra cosa distinta", entonces lo único que queda es "bueno... bien... seguiremos con lo nuevo entonces".

¿Qué vector es más sencillo de atacar: el tecnológico o el humano?

Esto es una opinión puramente personal, pero yo creo que el más sencillo es la tecnología porque siempre está encendida, siempre está ahí, necesita parches, necesita atención...

Paradójicamente, los seres humanos son el eslabón más fuerte y a la vez más débil de la ciberseguridad, pero pueden ver cosas que las máquinas no. Eso sí, los humanos tienen que estar bien equipados. Hay que darles las herramientas y la formación adecuadas.

Las máquinas simplemente están ahí. Y si están ahí todo el tiempo, abiertas a Internet, sin registros de seguridad o con una seguridad muy débil o falta de atención, entonces seguro que vas a tener problemas. Si alguien no ha parcheado una VPN o algo por el estilo, vas a tener problemas. Seguro.

He visto más y mayores problemas por ataques a la tecnología que por ataques a las personas. Y eso ha ocurrido tanto desde el punto de vista de daño financiero como del impacto en un servicio o compañía.

La ciberseguridad es la manifestación de una tecnología bien diseñada y entregada, lo correcto sería disponer de procesos para detener los problemas antes de que lo sean.

¿Qué oipina sobre BYOD como origen de vulnerabilidades?

Sé que hay soluciones en el mercado para mitigar el problema y hacer que todo sea más seguro. Además, con una clasificación y control de datos adecuados, un *sandboxing* apropiado y el uso de máquinas virtuales, estoy seguro de que funcionará.

Pero, personalmente, no me gusta. Reconozco que soy un poco de la vieja escuela en esto. Me gustan las cosas bajo mi control, para poder entender correctamente cuál es mi estado en todo momento. Y si entiendo cuál es mi estado, entiendo cuál puede ser mi vector de ataque y qué tamaño tiene mi superficie de ataque.

¿Cómo impacta la virtualización a la ciberseguridad?

Creo que es algo realmente bueno. Ofrece un control mucho mayor, así como la posibilidad de elaborar las previsiones de gasto. Supone menos esfuerzo, sobre todo en lo que se refiere a la recuperación de desastres y cosas por el estilo.

Por ejemplo, actualmente trabajo en un entorno totalmente virtualizado. No tenemos nada *on-premise*. Todos tenemos portátiles y podemos trabajar en cualquier lugar, con todos los controles adecuados. El problema sería si Microsoft se cayese, si AWS, una vez más, pasara a sus servidores en Virginia durante un tiempo, o cualquier cosa por el estilo.

Pero a mí me gusta el hecho de poder definir la infraestructura como código, tener una arquitectura debidamente acordada, bien construida, y pulsar un botón para que haga lo que debe hacer. Y cuando acaba, simplemente se apaga y desaparece.

> **Además, es muy importante trabajar de forma muy estrecha con el departamento legal y comercial**

¿Y en cuanto a la computación cuántica?

Efectivamente, la computación cuántica puede tener impacto en las iniciativas de seguridad. Por suerte, aparentemente hay dos algoritmos resistentes al *cracking* cuántico. Cuando finalmente salga a la luz, creo que va a generar un gran cambio en la forma de defenderse.

La forma en que lo veo es que va a estar mucho más basada en los dispositivos, con *tokens* que viajarán de aquí a allá. Pero si un *token* se ve comprometido, es solo un *token*. Realmente no importa. De lo que se trata realmente es de lo que hay en el teléfono o en el portátil y cómo se puede mantener segura esa información.

> **La ciberseguridad se basa en el concepto CIA: confidentiality, integrity, availability**

¿Qué impacto cree que tienen las redes sociales en cuanto a que la ciberseguridad, incentivando ataques debido a que van formado opiniones en poblaciones enteras?

Uno de los grandes peligros de las redes sociales es que pueden ir formando opinión en poblaciones enteras. Este es un problema importante que solo se ve en las redes sociales, debido al fácil acceso que la gente tiene a ellas.

En su día critiqué el ecosistema de Twitter, porque cuando nos atacaron en Travelex, aparecieron una serie de supuestos profesionales de la ciberseguridad que buscaban ayudar a su carrera con el incidente. En realidad, la ciberseguridad se basa en el concepto CIA: *confidentiality, integrity, availability*. Y yo me pregunto ¿cuánta integridad tienen estas personas y sus acciones dentro del área de la ciberseguridad?

Lo último que alguien necesita en medio de un ataque global de *ransomware*, es algún temerario alocado de Twitter diciendo: "Sé cómo sucedió esto. Sé esto...sé aquello...". Saliendo en la televisión y haciendo tanto ruido que, al final, se traduce aún en más problemas para las personas que están tratando desesperadamente de recuperar el control de su red. «

Retos del buen gobierno de la ciberseguridad

ALBERTO LÓPEZ

CISO en Solaria Energía

SOLARIA

solariaenergia.com

ENTORNOS CADA VEZ MÁS AMPLIOS Y CAMBIANTES

Personas, procesos y tecnología. No perdamos de vista en ningún momento estos tres pilares fundamentales para lograr en nuestras empresas, y en la sociedad en general, un buen gobierno de la ciberseguridad. Pero hay una variable, trasversal a estas bases, que es constante en el tiempo: la continua aparición de riesgos que debemos afrontar y mitigar.

En el ámbito de la ciberseguridad, cuando hablamos de riesgos aún persiste la errónea creencia de que se trata de una cuestión centrada eminentemente en la parte técnica. En absoluto. Los riesgos pueden ser técnicos, de gestión, estratégicos, etc.

El buen gobierno de la ciberseguridad debe tener en consideración que estamos ante un escenario global altamente complejo y dinámico, que, además, está aumentando de forma exponencial.

Hay que tomar conciencia de que la ciberseguridad de las empresas puede tener una afección en la sociedad, comportando riesgos que pueden derivar en un elevado impacto en los bienes y derechos de terceros. Sin duda se trata de un reto que debe ser afrontado desde "ayer".

El gobierno de la ciberseguridad no es una labor sencilla ni estática. La empresa, los responsables de esta, poseen una responsabilidad y ejercen unas prácticas con el objetivo de proporcionar una dirección estratégica adecuada en todo momento para alcanzar y asegurar los objetivos minimizando a su vez los riesgos.

> **Personas, procesos y tecnología. No perdamos de vista en ningún momento estos tres pilares fundamentales**

Esto es lo que conforma el gobierno corporativo, canalizado por la alta dirección, y la ciberseguridad debe (o debería) ser parte integral de este gobierno corporativo. Sin duda, este es un reto para muchos CISO.

Si nos centramos en cuestiones concretas, una protección eficiente, sea a nivel de gestión o a nivel técnico, solo se puede llevar a cabo si se implantan estrategias adecuadas en función de cada negocio y del gobierno corporativo. No podemos aplicar los mismos criterios y estrategias a todas las empresas.

Por ello, los retos son muchos y variados: tratar de simplificar y optimizar la ciberseguridad, evaluar riesgos continuamente, velar en todo momento por la continuidad de la empresa y por su reputación, etc. De no ser así, puede desembocar en un daño económico, operativo y reputacional irreversible para las organizaciones.

OBJETIVOS Y RETOS DE LA CIBERSEGURIDAD

El Gobierno de la Ciberseguridad se ha convertido en una prioridad para cualquier administración pública, empresa, u organización en general que preste servicios digitales y, por tanto, haga un uso masivo de las tecnologías de la información y de las comunicaciones. No se concibe hoy día un gobierno corporativo que no considere el gobierno de la ciberseguridad, aunque solo sea a efectos de identificar y valorar los riesgos específicos de esta materia. De hecho, si no son gestionados pueden llegar a comprometer la credibilidad y confianza de los ciudadanos, e incluso generar importantes pérdidas económicas que afecten a su viabilidad futura.

Entre los objetivos principales del buen gobierno de la ciberseguridad podemos citar:

La determinación de la estrategia, funciones y capacidades de ciberseguridad a diseñar e implementar en la organización alineadas con los objetivos estratégicos del negocio.

La gestión del riesgo.

La aportación de valor y el retorno de inversión.

La evaluación, medición y mejora continua de los indicadores de estado de ciberseguridad.

Los planes y programas de proyectos a abordar.

El cumplimiento legislativo y normativo.

Considerando estos objetivos tan ambiciosos, los retos a afrontar no se quedan atrás. Entre ellos podemos destacar:

La complejidad de conseguir que la ciberseguridad tenga visibilidad e importancia para la alta capa directiva, e incluso forme parte de los comités de dirección.

El aumento exponencial de la presencia en Internet de las organizaciones, lo que conlleva mayor exposición ante ataques de ciberseguridad.

La gestión de riesgos poco madura y con poca referencia de modelos de éxito.

La falta de buenas prácticas en seguridad en el diseño y, por defecto, de muchas tecnologías y soluciones TIC.

La volatilidad de las tecnologías y su rápida evolución y cambio constante.

Las interrelaciones y dependencias con sistemas y redes de socios, colaboradores y/o proveedores que no siempre son seguros.

La evolución, el aumento exponencial y la sofisticación de las amenazas, ataques de ciberseguridad y actividades criminales.

Lo prolija y compleja que es la legislación en materia de ciberseguridad.

La falta de concienciación, formación de los usuarios.

La enorme escasez de profesionales de ciberseguridad, tanto a nivel europeo como mundial.

Estos retos requieren una aproximación inteligente y por partes, que se debe cumplimentar con un liderazgo y mentalidad abierta al cambio, resiliente, ambiciosa y humilde a la vez. Esto es lo que permita afrontarlos de forma diligente sin caer en el desaliento.»

ESTHER MUÑOZ FUENTES

Subdirectora General de Ciberseguridad, protección de datos y privacidad

MADRID DIGITAL

comunidad.madrid

> **“Ya no se concibe un gobierno corporativo que no considere el gobierno de la ciberseguridad**

JESÚS MÉRIDA

Chief Information Security Officer

IBERIA

www.iberia.com

PRINCIPIOS BÁSICOS DE UN BUEN GOBIERNO DE SEGURIDAD

Cuando nos preguntamos cuales son los principios de un buen gobierno de la ciberseguridad podemos encontrar la respuesta en alguno de los numerosos marcos de referencia que existen a nivel internacional —como NIST, ISO/IEC 27001— o incluso a escala nacional, como es el caso del Esquema Nacional de Seguridad. Todos ellos apuntan una serie de pistas acerca del modo adecuado de establecer dicho gobierno. Pero no olvidemos que cada empresa es un mundo y, como tal, seguramente no podremos coger ninguno de estos marcos como si de una receta mágica se tratara.

Aunque el enfoque habitual suele ser estratégico, y desde mi punto de vista es lo correcto, también es cierto que se deberían incluir, como si de ingredientes secretos se tratara, una serie de pinceladas tácticas que habría que tener en cuenta en casi todas las situaciones:

Entender el negocio o, más bien, los patrones culturales y de comportamiento tanto a nivel organizativo como individual de nuestras compañías. El objetivo debería pasar por establecer patrones de negocio que nos ayuden a identificar y proteger adecuadamente nuestros datos.

> **Aunque el enfoque suele ser estratégico, se deberían incluir una serie de pinceladas tácticas en casi todas las situaciones**

Otra práctica aconsejable es realizar un buen **caso de negocio** de ciberseguridad y establecer claramente el apetito del riesgo. Es importante que esto no se desarrolle de forma aislada, desde la disciplina de seguridad o de TI, sino haciendo comprender a la organización que el riesgo de ciberseguridad es compartido. Es más, hacer entender que todas las áreas de la compañía, independientemente de su actividad, deben ayudar a reducirlo, asumiendo una parte de la responsabilidad conjunta. Además, este caso debe ser también validado por negocio en su máxima representación, como puede ser el comité de dirección.

Además de esto, también debemos **garantizar la seguridad** en los procesos y estructuras de negocio, estableciendo para ello una serie de objetivos claros y alcanzables. Además, es importante asegurándonos de que la ciberseguridad participa por derecho propio en todos estos procesos, desde la concepción y el diseño. Para ello, debe de estar correctamente representada a lo largo y ancho del negocio, en los distintos grupos internos y en posiciones de liderazgo.

Por último, una práctica importante es ser capaces de **evolucionar** constantemente todo lo anterior. Seguramente esto es sencillo de decir, pero quizá sea lo más difícil de llevar a cabo.

En cualquier caso, la base de un correcto gobierno de ciberseguridad es dudar de todo, y revisar constantemente nuestros pilares y bases en busca del posible error o de la ansiada mejora. «

XXIV JORNADA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN

17 NOV

isms forum

www.ismsforum.es

GUILLEM COLOM PIELLA

Codirector de THIBER, the cybersecurity think tank

THIBER

thiber.org

Lecciones de ciberguerra en Ucrania

INTEGRAR EL ELEMENTO INFORMATIVO

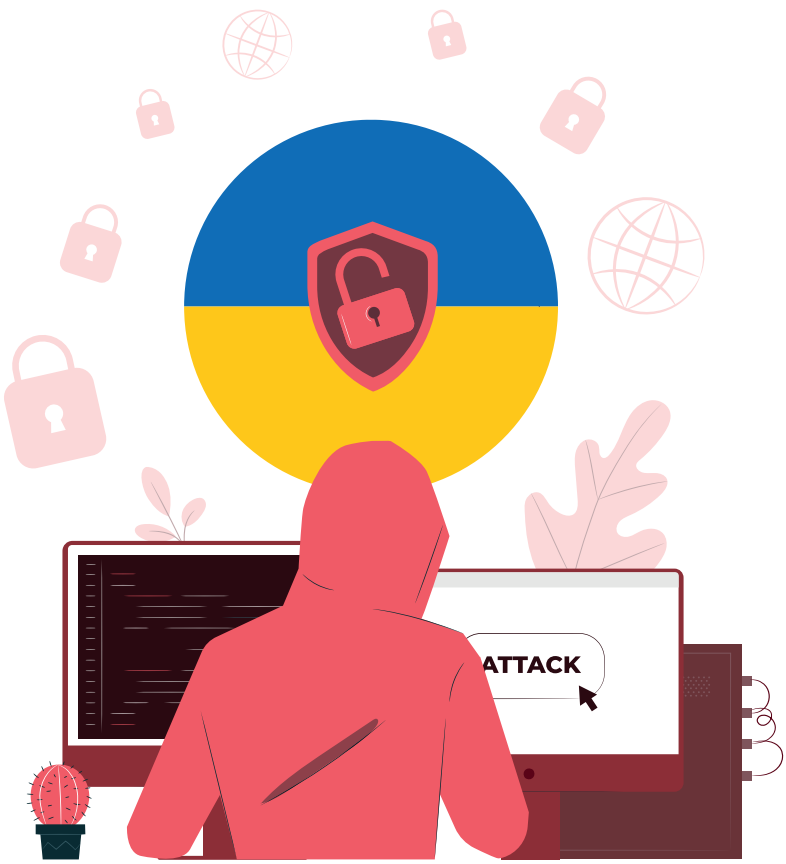
El 24 de febrero de 2022 será recordado porque Rusia inició la invasión de Ucrania. Bajo el pretexto de desmilitarizar y "desnazificar" el país, esta guerra está desarrollándose según unos parámetros que nadie había previsto. La mayoría de los estrategas asumían que el elemento informativo ruso (que combina la dimensión técnica en el espectro cibernético y electromagnético con la psicológica, vinculada con la propaganda y la desinformación) tendría un papel predominante. Especialmente porque desde la invasión de Georgia (2008) venía potenciando este elemento como parte integral de sus "guerras de nueva generación".

En este sentido, se asumía que Moscú prepararía la invasión con un repunte de las acciones informativas contra el régimen ucraniano, la población rusa y la opinión pública internacional. Este se combinaría con una amplia gama de ciberataques de distinto perfil contra infraestructuras críticas y servicios esenciales. Por su parte, las operaciones militares arrancarían con la degradación —física y/o lógica— de la arquitectura de mando y control, así como del sistema de defensa aérea ucranianos.

Todo ello serviría como demostración del poder ruso para modelar las narrativas, erosionar la voluntad del liderazgo y pueblo ucraniano, generar miedo y caos, romper su ciclo de toma de decisiones, aislar los estados mayores de las fuerzas desplegadas y facilitar el logro de la superioridad aérea.

Por su parte, las unidades rusas operarían —como ya se observó en Ucrania o en Siria durante los años anteriores— bajo una importante cobertura electrónica para dificultar la maniobra ucraniana. Todo ello se combinaría con una señalización nuclear y cibernética para controlar la escalada y dificultar cualquier intervención internacional, así como operaciones informativas para degradar la capacidad militar adversaria, minar su voluntad de resistencia y mantener desconcertada a la opinión pública internacional.

Ello también requeriría que la operación se planteara como un "golpe de mano" para alcanzar la situación final deseada antes de que la Comunidad Internacional comprendiera el alcance real de la situación y planteara algún tipo de respuesta coordinada…como finalmente ha sucedido.



DESINFORMACIÓN

Quizás, el objetivo inicial era este: una operación de "choque y pavor" contra el presidente Zelenski, similar al asalto al palacio presidencial de Afganistán (1979) y amparada por una potente campaña informativa para confundir al mundo sobre las intenciones rusas hasta que el Kremlin hubiera alcanzado sus objetivos… Una operación de zona gris casi de manual. Algo que había logrado con éxito seis años antes, cuando unidades —no marcadas— y actores locales tomaron Crimea bajo la atónita mirada de la Comunidad Internacional.

Explotando los clivajes sociopolíticos de la región y lanzando una campaña multicanal de desinformación dentro y fuera de Ucrania, Moscú fue capaz de ocultar sus objetivos y negar de manera plausible sus responsabilidades hasta consumar la invasión.

En otras palabras, cualquier estratega asumía que Moscú integraría desde el primer momento, y a todos los niveles, el elemento informativo, tal y como hizo por primera vez en Georgia y continuó haciendo en Crimea, el Donbas o en

Siria. Parecía lógico: entraba dentro de la tradición soviética de la *maskirovka* y la desinformación; estaba en línea con los pilares de sus "guerras de nueva generación"; el general Gerasimov había alertado de su relevancia múltiples veces desde la Jefatura de Estado Mayor de la Defensa rusa; y las lecciones identificadas de sus intervenciones recientes indicaban que así sería. Quizás, este fue su error. Y es que, paradójicamente, Moscú parece haber acabado combatiendo una guerra del siglo XX mientras que Ucrania está librando un conflicto del siglo XXI, en línea con lo que varios teóricos habían planteado años atrás. De hecho, el elemento cibernético ruso parece haber sido bastante anecdótico. ¿Significa esto que Rusia no ha intentado emplear sus capacidades? ¿Implica que no ha existido ninguna ciberguerra? Al contrario. Tal y como bien expone nuestro compañero Pedro López en otro artículo de esta revista, parece haberse producido de una manera distinta de cómo se esperaba a nivel estratégico-militar.

CIBERCAPACIDADES

En este sentido, todavía es muy pronto para extraer lecciones de esta guerra que puedan informar sobre el desarrollo de estrategias futuras. De hecho, el mediocre desempeño ruso en el espacio informativo no debe llevarnos a minusvalorar su potencial en las guerras futuras, sino al contrario. Asuntos como la imposibilidad de degradar el sistema de mando y control ucraniano, la escasez de comunicaciones seguras, el potencial empleo de sus ciberguerreros para mantener operativa su arquitectura de mando y control, la posible sobreestimación de sus cibercapacidades, su incapacidad en materia de guerra electrónica, el mediocre desempeño de su maquinaria de desinformación, el limitado impacto de las ciberarmas utilizadas o la virtual desaparición de ciertos *proxies* que permitían proyectar el poder ruso dificultando la responsabilidad podrían indicar la falta de madurez rusa. Algo que se complementaría con el pobre desempeño ruso en el campo de batalla.

Sin embargo, también podrían sugerir que el *modus operandi* ruso ya era conocido y se han utilizado todos los medios posibles para erosionar su capacidad:

Hasta el mismo día de la invasión, Moscú utilizó todos sus altavoces directos e indirectos para negar que su despliegue de fuerzas cerca de las fronteras ucranianas fuera coercitivo. Algo que era repetidamente refutado por la inteligencia estadounidense y británica.

Cuando arrancaron las hostilidades, Rusia atacó las infraestructuras críticas y los servicios esenciales del país. Sin embargo, su resiliencia había aumentado notablemente tras seis años de experimentar este tipo de ataques en la zona gris.

Además, parece que las capacidades de guerra electrónica que Moscú llevó al conflicto se utilizaron de manera muy limitada debido a la escasez de comunicaciones seguras rusas, y fueron rápidamente diezmadas por ataques de precisión ucranianos. Ataques cuya selección de objetivos era proporcionada por Estados Unidos y sus aliados. De hecho, parece que la colaboración de Washington, las grandes tecnológicas y los grupos *hacktivistas* que se han posicionado a favor de Ucrania han sido esenciales para minimizar el impacto de los ciberataques rusos a la vez que se degradaba su capacidad militar sobre el terreno.

La información de la que disponemos es todavía parcial y muy incompleta, aunque con el tiempo se irán conociendo más detalles sobre esta contienda. Sin embargo, no debemos olvidar que las guerras presentes y futuras se libran en todos los dominios (terrestre, naval, aéreo, espacial, cibernético o cognitivo) y que el elemento cibernético es uno de los componentes para maniobrar en el campo de batalla y contribuir al éxito de la operación. Si un objetivo puede ser batido más fácilmente con una bomba o un misil, lo lógico es que así sea. Se trata de uno de los principios de la guerra: la economía de medios.

> **El mediocre desempeño ruso en el espacio informativo no debe llevarnos a minusvalorar su potencial**

LA ZONA GRIS

Sin embargo, quedan dos cuestiones pendientes: Primero, ¿cómo puede ser que Moscú no haya escalado de manera deliberada utilizando medios cibernéticos contra infraestructuras críticas y servicios esenciales de terceros países? Especialmente cuando, desde el primer momento, puso encima de la mesa el arma absoluta para señalizar sus intenciones. Segundo, y quizás más importante, ¿puede que el entorno natural donde mejor se mueve lo ciber sea en la zona gris?

Si algo hemos visto durante los últimos años es como este espacio ambiguo, situado debajo del umbral del conflicto armado, permite utilizar una amplia gama de herramientas del poder nacional para explotar las vulnerabilidades sistémicas de la sociedad adversaria. La ambigüedad, anonimidad, asimetría, economía y ubicuidad características del ciberespacio permiten proyectar el poder de manera asimétrica dificultando su identificación, atribución y respuesta.

Quizás no se trata del "ciber Pearl Harbor" vaticinado por muchos hace unos años, pero a medida que vamos a un mundo más inestable veremos cada vez más acciones de este tipo contra nuestras sociedades.

La guerra de Ucrania empezó en 2014 con una zona gris rusa que ha escalado hacia un conflicto convencional y una ciberguerra que, quizás, no es convencional. Tenemos por delante muchas lecciones que aprender. «

PEDRO LÓPEZ SÁEZ

Director del Máster en Protección de Datos y Seguridad de la Información UCM

UCM

¿Ha empezado la ciberguerra?

EVALUAR EL NIVEL DE PREPARACIÓN A NIVEL PAÍS

Si vis pacem, para bellum (si quieres la paz, prepárate para la guerra), máxima atribuida a Flavio Vegecio en el siglo IV. Aunque las armas, ejércitos y flotas de los romanos están obsoletas, los principios de dominación territorial que perseguían se mantienen. A los combates por tierra y mar, durante el siglo XX se añadió también el espacio aéreo para las operaciones militares y más recientemente también se ha reconocido la importancia del espacio y del ciberespacio.

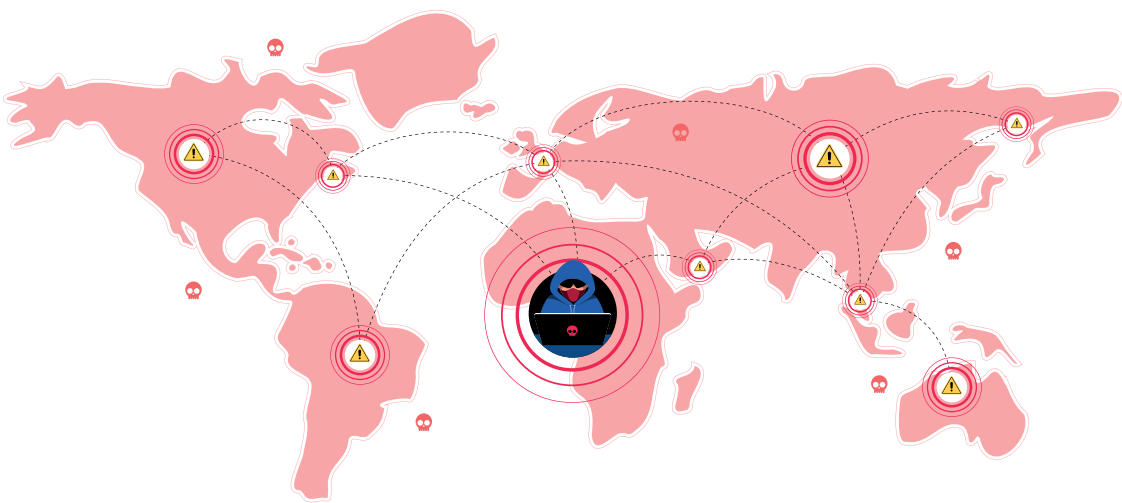
El espacio y ciberespacio comparten la característica de quedar fuera de la geografía de algún país, y también comparten una extraordinaria capacidad para recoger información para labores de inteligencia con la que conducir con éxito operaciones en ese mismo dominio o en cualquiera de los demás (tierra, mar y aire). Sin embargo, el ciberespacio, como quinto dominio de operaciones, resulta completamente singular.

El conflicto de Ucrania ofrece un excelente ejemplo para comprender la relevancia que tiene el ciberespacio como teatro de operaciones. Según los datos recogidos por Paolo Passeri en Hackmaggedon, entre enero y marzo de 2022 los ciberataques con motivaciones de ciberguerra aumentaron un 400% y los vinculados al *hacktivismo* un 500%.

Esta es una de las características propias del ciberespacio como dominio de operaciones: la opacidad. En el ciberespacio es difícil distinguir a las fuerzas regulares de las irregulares, de grupos mercenarios o meramente oportunistas. Por ejemplo, Anonymous declaró oficialmente la ciberguerra contra el gobierno ruso y su presidente y, por su parte, el Conti Team —especializado en *ransomware*— prometió represalias en caso de que "los belicistas occidentales" atacasen infraestructuras críticas rusas.

El ministro de Transformación Digital de Ucrania, **Mykhaylo Fedorov**, realizó un llamamiento para reclutar voluntarios con diferentes talentos digitales para la guerra, con el que formar un ejército de TI que podría tener entre 200.000 y 400.000 efectivos. No obstante, para su ciberdefensa Ucrania ya cuenta con el apoyo de CERTs de EE.UU., la UE y la OTAN. En concreto, el Comando Cibernético norteamericano, bajo el mando del General Nakasone, también director de la Agencia de Seguridad Nacional (NSA), ha reconocido estar prestando apoyo analítico remoto y realizando actividades de defensa de la red en Ucrania.

Además de medios oficiales e "independientes", diversas empresas privadas, especialmente norteamericanas, también se han posicionado contra las ciberoperaciones rusas o prorusas. Por ejemplo, Microsoft colabora con funcionarios de ciberseguridad y empresas privadas ucranianos en la defensa contra ciberataques, Meta o Youtube han prohibido los anuncios de medios estatales rusos y han bloqueado la capacidad de monetización de sus cuentas, y el servicio de internet vía satélite de Starlink ha enviado antenas a Ucrania para que el país pueda seguir conectado a pesar de los ataques a su infraestructura de comunicaciones.



»CIBERGUERRA

Rusia lleva realizando ciberoperaciones y acciones de ciberguerra desde hace varios años. En 2007 atacó *webs* gubernamentales en Estonia y dejó sin servicio *online* a algunos bancos del país durante horas. Aunque el daño físico causado no fue catastrófico, Estonia se desconectó de Internet para recuperarse y se produjo una gran alarma social. La OTAN estableció en Tallin su Centro de Excelencia Cooperativa de Ciberdefensa.

Los ejemplos más recientes de ciberguerra rusa pueden observarse, por ejemplo, en el uso combinado de ciberoperaciones y de acciones militares convencionales en el caso de Georgia en 2008 y de Ucrania en 2014. Un estudio reciente de **Emelie Karlsson**, de la Universidad de Uppsala, considera que en estos casos el uso de la ciberguerra no fue adecuado desde el punto de vista de la diplomacia coercitiva, ya que no se permitió obtener concesiones políticas de ningún tipo e incluso se incentivó a que estos países se planteasen un acercamiento a la OTAN. No obstante, sí que tuvo cierto impacto desde el punto de vista operativo-militar, especialmente en el campo psicológico, afectando a la moral del adversario.

Más recientemente, según un informe especial elaborado por Microsoft, las ciberoperaciones de Rusia ya supusieron que, entre junio de 2020 y junio de 2021, Ucrania fuera el segundo país que sufría más ciberataques de todo el planeta, solo por detrás de EE.UU. Por tanto, se realizó una intensa actividad de preposicionamiento contra organizaciones ucranianas y sus posibles aliados con el fin de recopilar información de inteligencia y conseguir un acceso continuado a las redes que facilitara ataques destructivos en caso necesario.

Otro ejemplo: justo antes de la invasión, los satélites de Viasat y Starlink sufrieron un ciberataque que provocó cortes de Internet en varios países europeos. Aunque se trataba de plataformas civiles, las fuerzas y cuerpos de seguridad ucranianos utilizaban estos operadores para sus comunicaciones. Además, de acuerdo con Kaspersky, la semana en la que se produjo la invasión, los ataques DDoS alcanzaron máximos históricos, llegando a multiplicar por 30 el mínimo del último año. Y ya iniciado el despliegue militar, los ciberataques se han dirigido especialmente contra infraestructuras críticas ucranianas como la red eléctrica, sus centrales nucleares y sus telecomunicaciones, utilizando familias de *malware* destructivo que se propaga al estilo del *ramsomware*. En ocasiones se empleaba información sobre la guerra como cebo, borrando datos e incluso impidiendo el arranque de los dispositivos afectados.

»UN RIESGO REAL

Para entender las operaciones de Rusia en el ciberespacio es muy relevante el concepto ruso de "confrontación por la información" o IPb (*informatsionnoye protivoborstvo*). Un informe de la Agencia de Inteligencia para la Defensa (DIA) norteamericana describe este término como la confluencia de los ámbitos de información diplomática, económica, militar, política, cultural, social y religiosa. Básicamente se busca influir con efectos técnico-informativos (ciber-operaciones) e informativo-psicológicos: intentos de alterar las percepciones o manipular el comportamiento de audiencias objetivo a favor de los intereses gubernamentales rusos, teniendo un carácter más estratégico y de largo plazo.

Dado que Rusia contempla el uso de la ciberguerra contra los países que considera hostiles, tanto en tiempo de paz como durante los conflictos armados, es conveniente evaluar cuidadosamente el nivel de preparación de nuestro entorno. Nos encontramos ante un riesgo real.

Según una auditoría del Tribunal de Cuentas Europeo, ha aumentado mucho el número de ciberataques a instituciones de la UE, concluyendo que la preparación actual no se encuentra a la altura que exigen las amenazas actuales. Recientemente, el CNI ha atribuido a Rusia ciberataques diarios de muy alta peligrosidad contra España, y el precio de los seguros contra ciberriesgos ha aumentado notablemente desde el inicio de la guerra de Ucrania.

Determinar el grado de preparación de un país no es sencillo. La Kennedy School de la Universidad de Harvard publicó en 2020 el índice de ciberpotencias globales (National Cyber Power Index). Posiblemente es el estudio más amplio, minucioso y reciente sobre las intenciones y capacidades relativas al ciberespacio de diversos países. En este índice, EE.UU., China y Reino Unido ocupan el podio, mientras que Rusia aparece en el cuarto lugar. Por su parte, España ocupa el puesto número doce, y es el cuarto país europeo en el *ranking*, por detrás de Países Bajos, Francia y Alemania. No obstante, esta clasificación de 2020 puede no ser del todo representativa, pues las actividades en el ciberespacio suelen ser eminentemente opacas, tanto en lo que se refiere a agresiones como a las capacidades defensivas. El pasado mes de abril, el Centro de Excelencia de Ciberdefensa de la OTAN celebró sus ejercicios de ciberdefensa anuales (Locked Shields 2022), en los que participaron 2000 militares de 32 países. El equipo español acabó en la última posición.

Esperemos que el anunciado plan nacional de ciberseguridad, y su esperada dotación presupuestaria de 1000 millones de euros, permita desarrollar las cibercapacidades necesarias para afrontar el contexto en el que ya nos encontramos. La guerra convencional en Ucrania concluirá, esperemos que cuanto antes. Sin embargo, es previsible que la utilización de la ciberguerra como instrumento político se intensifique con el paso del tiempo, por parte de Rusia y de otras ciberpotencias.

Si queremos la paz en el ciberespacio, debemos prepararnos para la ciberguerra. «

CARLOS ALBERTO SÁIZ PEÑA

Socio de Ecix Group
Vicepresidente de ISMS Forum y Director del Data Privacy Institute

ISMS FORUM

ismsforum.es

Implantar un sistema de *cybercompliance*

RETOS REGULATORIOS EN CIBERSEGURIDAD

El panorama regulatorio en ciberseguridad es complejo y lo va a ser más en los próximos años. Por este motivo, las organizaciones deben dotarse de un sistema de cybercompliance que les ayude a mitigar sus riesgos de cumplimiento y fortalecer su fiabilidad como compañía de cara al mercado y a terceras partes.

Vivimos un auténtico frenesí normativo en el ámbito tecnológico y, por extensión, en todo lo referente a la protección de la información, las infraestructuras y los servicios digitales: la ciberseguridad. Hace años, la regulación fue considerada en el entorno privado como una buena palanca para promover las primeras grandes inversiones en seguridad de la información. En la actualidad, los datos sobre ciberamenazas y ciberdelincuencia son alarmantes para cualquier organización pública o privada, y refuerzan el discurso de los profesionales para seguir concienciando en la necesidad de mejorar en este ámbito.

No podemos olvidar que no se trata de la protección por la protección, sino de salvaguardar los derechos que pueden verse comprometidos o lesionados detrás de toda esa tecnología. Cuando hablamos de ciberseguridad, estamos hablando de proteger el interés del Estado, el derecho de acceso a servicios públicos, a la protección de datos, a la propiedad —también a la de carácter intelectual—, a la información, al honor y la intimidad, etc.

Cumplir con la normativa de ciberseguridad no solo es una tarea necesaria para evitar multas, sino una manera de sistematizar los esquemas de protección de los derechos que organizaciones y personas ostentan en una auténtica jungla digital.

La dificultad que esto entraña es clara: hay muchas normas, todas ellas con muchas diferencias en cuanto al alcance, obligaciones, sistemas y tecnologías...; además de muchas autoridades e instituciones con diferentes competencias y funciones. Por ello, aunque hay muchos retos asociados a implantar y mantener un sistema de *cybercompliance*, es muy importante porque ayuda a que una compañía:

- Conozca sus riesgos normativos.
- Proteja mejor sus activos.
- Sea fiable en el mercado.
- Evite multas o sanciones.
- Tenga una alineación equilibrada entre negocio y cumplimiento.

CYBERCOMPLIANCE MAPPING

Puede parecer obvio, pero no lo es. Es necesario que las organizaciones trabajen en crear y actualizar de manera constante un mapa de riesgos normativos que contenga el universo de requisitos regulatorios y legales a los que se enfrenta. Las "obligaciones" y los "compromisos" son

muchos y tienen diferentes alcances, por eso lo ideal es que dentro de ese mapa incluyamos lo siguiente:

- Normas, tanto nacionales (LOPDGDD, ENS, LPIC, Real Decreto 43/2021, Real Decreto-ley 12/2018, Compliance Penal, Ley de secretos empresariales, etc.) como internacionales (RGPD, Directiva NIS, SOX, futuro Reglamento Ciberseguridad, Directiva Servicios Digitales, Data Act, etc.) o sectoriales (eIDAS, DORA, 5G, MiCA, PSD2, etc.).
- Obligaciones contractuales, cuyo incumplimiento puede tener un mayor impacto en términos de responsabilidades, penalizaciones, demandas, etc. Por ejemplo, el cumplimiento de SLA, control de licencias, obligaciones de seguridad de servicios cloud, etc.
- Estándares y certificaciones: ISO 27001, ISO 27701, ISO 37301, ENS, PCI-DSS, etc.
- Normativa y procedimientos internos, como el código de uso de dispositivos, clasificación de información, gestión de incidentes de seguridad y datos, protocolo forense e investigaciones, *third party compliance,* etc.

» CONSTRUIR UN SISTEMA DE CYBERCOMPLIANCE

Es importante manejar un sistema de cumplimiento en ciberseguridad como un sistema de gestión clásico conforme al Ciclo de *Deming*: Plan-Do-Check-Act. Dejando de lado los aspectos más evidentes acerca de cómo se debe conformar ese sistema, me gustaría resaltar otros que a veces pasan inadvertidos y considero muy relevantes. En este sentido, un sistema de *cybercompliance* debe contar con:

- Un canal de observatorio normativo que le ayude a anticiparse a las normas que vendrán y que, de forma preventiva, le permita analizar cómo le va a impactar. Por ejemplo, la futura publicación de una ley cuando está en estado de proyecto o anteproyecto.
- La capacidad de escalar y absorber novedades normativas y nuevos compromisos obligatorios dentro de un mismo y único sistema de gestión de *cybercompliance*, y huir de crear marcos normativos paralelos de gestión diferenciada.
- Un inventario completo y claro de las instituciones, sus competencias y datos de contacto, (especialmente de reguladores y autoridades): CCN, INCIBE, CNPIC, AEPD, ENISA, EDPS, SEDIA, Banco de España, CNMV, CNMC, Fiscalía, Fuerzas y Cuerpos de Seguridad, etc.). Además de un inventario actualizado *Legal Risk Mapping.*
- Metodologías comunes de análisis de riesgo legal (por ejemplo, ISO 31022) para todos los requisitos normativos a los que enfrentarse y así poder obtener niveles de riesgo comparables.
- Herramientas de radar e información sobre los impactos de incumplimiento que sean aplicables, es decir, conocer de forma actualizada qué sanciones se han puesto, a qué tipo de empresa, por qué incumplimiento concreto, etc. No es posible realizar buenos cálculos en un análisis de riesgo legal si únicamente nos fijamos en cómo mejorar nuestro nivel de vulnerabilidad (mejor cumplimiento) y no prestamos atención al impacto, ni a la probabilidad.
- La posibilidad de generar indicadores y métricas asociadas a los niveles de riesgo. Es necesario medir la eficacia de las medidas y controles de cumplimiento, y definir labores de supervisión más allá de esperar a que Auditoría venga a realizar su examen. Todo ello mejorará los niveles de report hacia dirección/consejo, y ayudará a tomar mejores decisiones en cuanto a la mitigación de riesgos normativos.
- Expertos y recursos adecuados. La tecnificación de la ciberseguridad no solo ha llegado a los CISO y los equipos técnicos, es necesaria una mayor cualificación legal de profesionales en el ámbito de la ciberseguridad. El incremento de normas, la complejidad de los diferentes marcos regulatorios y el reto de gestionar de manera eficiente todo ello en una organización requieren de personas preparadas a tal efecto.

> **Es necesario crear un mapa de riesgos normativos que contenga el universo de requisitos regulatorios y legales**

- Uso de la inteligencia artificial y de herramientas *legaltech* para automatizar tareas repetitivas, análisis de documentación y riesgos, información para ayuda a la toma de decisión, etc. Pensemos en cuántos NDA firmamos al año, contratos de prestación de servicios ordinarios, contratos de encargo de tratamiento iguales, cláusulas de cesión de derechos de propiedad intelectual similares, etc. Todo ello conlleva cientos o miles de horas de trabajo de personas donde apenas existe una aportación de valor real. Resulta fundamental llevar la transformación digital también a esta área y utilizar la tecnología ya existente para gestionar un sistema de cybercompliance de manera más eficaz.
- Un *governance* interno muy bien definido entre CISO, DPO, Asesoría Jurídica, *Compliance*, Auditoría, Control Interno, etc., donde los nombramientos y las competencias estén claras y se eviten solapamientos, fricciones innecesarias y conflictos de interés.
- Un proceso de adopción cloud maduro y testeado. Los llamados *journey to cloud* se han llevado de manera rápida e imprecisa por muchas organizaciones. En este sentido, es importante definir muy bien las responsabilidades internas y externas que existen cuando se decide contratar cualquier servicio en modo *cloud*, definir muy bien los pasos cronológicamente y disponer de las tareas que cada área debe acometer en este sentido (propuesta, costes iniciales, facturación, riesgos, seguros, contratación, *data privacy*, migración, supervisión, auditoría, renovación, etc.). «

PARTNERS

Platinum Sponsors

aiwin · CLOUDFLARE · CROWDSTRIKE · Microsoft

PENTERA · Recorded Future · VECTRA · zscaler

Gold Sponsors

Akamai · aruba (a Hewlett Packard Enterprise company) · Check Point (Software Technologies Ltd.) · cipher (a Prosegur company) · cisco · WatchGuard | CYTOMIC

Delinea · DEVO · Forcepoint · FORTINET · HUAWEI · netskope · NEXTVISION & SecurityScorecard

NOZOMI NETWORKS · okta · paloalto NETWORKS · radware · riskrecon (mastercard) · NETWITNESS An RSA Business · S21sec

SentinelOne · sonatype · splunk> · TREND MICRO

Silver Sponsors

BioCatch · CYCOGNITO · proofpoint.

isms forum — INTERNATIONAL INFORMATION SECURITY COMMUNITY

www.ismsforum.es
@ISMSForum
ISMS Forum