FAQS - CIBERSEGURIDAD

(preguntas frecuentes sobre seguridad de la información)

ABSTRACT

El Grupo de Calidad y Seguridad de AUTELSI viene generando informes y guías de seguridad de la información. En esta ocasión, y mediante un formato de "pregunta y respuesta", trata de verbalizar una serie de cuestiones relevantes para que los no profesionales de la seguridad obtengan respuestas a preguntas que quizás se las hayan hecho en alguna ocasión.

AUTELSI - Grupo de Calidad y Seguridad

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)

Grupo de Trabajo de Calidad y Seguridad

Trabajo presentado el 18 de abril de 2023

Índice

Introducción

Desde la creación del Grupo de Seguridad de la asociación AUTELSI se vienen generando informes y guías de seguridad de la información. Estos documentos son elaborados por un amplio conjunto de profesionales de este ámbito, con formaciones y experiencias complementarias, para que sirvan de conocimiento y apoyo no sólo a otros profesionales de la seguridad de la información, sino también a otros roles relacionados e incluso a aquellos que comparten responsabilidad o dirigen jerárquicamente a estos.

En esta ocasión, el grupo mediante un formato de "pregunta y respuesta" trata de verbalizar una serie de cuestiones relevantes para que los no profesionales de la seguridad, obtengan respuestas a preguntas que quizás se hayan hecho en alguna ocasión.

En la elaboración del prontuario han colaborado profesionales de reconocido prestigio que desempeñan el rol de CIO (*Chief Information Officer*) o Responsable de Sistemas de Información. La selección de las preguntas que finalmente se han incluido y sus respuestas se ha realizado en el seno del grupo de seguridad de AUTELSI. Esperamos sean de ayuda.

Preguntas frecuentes sobre seguridad de la información

¿El uso de las tecnologías siempre acarrean riesgos?

Si, siempre. Ahora bien, la probabilidad de que se materialice una amenaza sobre esa tecnología y el impacto en el caso de que eso suceda, es lo que determina el nivel de riesgo.

A mí nunca me va a pasar nada. Hasta ahora nunca he sido objetivo de nadie. ¿Quién puede tener interés en atacarme a mí?

Cualquier empresa, por pequeña que sea, puede ser objetivo de un ataque. Desde un hacker hasta un empleado o colaborador (*insiders*) pueden tener interés en sacar información u obtener algún tipo de beneficio. Adicionalmente debes tener en cuenta que en ocasiones nos pueden atacar causándonos daños sin ser el objetivo final; como puente a un objetivo mayor o para encubrir su autoría. Además, para cumplir con ciertas regulaciones como el Reglamento europeo General de Protección de Datos (RGPD), es necesario realizar análisis de riesgos cuando se tratan datos de carácter personal, para tomar las medidas oportunas.

¿No existe una legislación europea en materia de seguridad y ciberataques?

Existe un Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado y modificado en mayo de este año. Este Código contiene la referencia a todo el marco jurídico en la materia, desde la propia Constitución Española a los principales Reglamentos Europeos aplicables, además de Leyes Orgánicas y Leyes, Reales Decretos, Resoluciones y Órdenes relacionadas con la Seguridad.

Se mencionan todas las normativas respecto a los siguientes aspectos: Seguridad Nacional, Protección de Infraestructuras Críticas, Seguridad Física, Respuesta a Incidentes de Seguridad, Ciberseguridad, Telecomunicaciones y usuarios, Protección de Datos Personales y Ciberdelincuencia.

¿Es necesario tener un departamento de seguridad?

Si utilizamos tecnologías de la información, si utilizamos ordenadores, alguien debe ocuparse de protegernos de los riesgos y de reaccionar lo más pronto posible ante la materialización de la amenaza y minimizar el impacto. Para realizar esas actividades - que implican prevención, detección, reacción y recuperación – es necesario tener profesionales que sepan llevar a cabo la práctica de la seguridad.

Tener profesionales no implica tener un departamento. Dependiendo de su tamaño y sus capacidades la empresa podrá: bien contar con profesionales propios especializados o que

compatibilicen esas actividades con otras (por ejemplo, con el mantenimiento de los ordenadores), o bien contar con servicios de seguridad externalizados total o parcialmente.

¿Es necesario disponer de un responsable de seguridad (CISO)?

Es absolutamente necesario, ya sea interno o en modo servicio, con total o parcial dedicación. Es imposible ejercer una práctica de la seguridad (tener seguridad) si no hay alguien que tenga esa responsabilidad. Las cosas no se hacen solas, ni se hacen sólo con buena voluntad.

Es necesario identificar las obligaciones en esta materia, establecer una estrategia, establecer unos principios (lo que se denomina la "postura de seguridad" de la empresa) desarrollar esa postura y dirigir la práctica. Estas, son algunas de las tareas que un CISO debe realizar.

¿Si trabajo para la administración tengo obligaciones de ciberseguridad? ¿y aunque expresamente no se indiquen en la licitación o adjudicación?

Si tu empresa trabaja para la Administración proveyendo productos o servicios en los que se maneje información digital tienes la obligación de cumplir el Esquema Nacional de Seguridad (ENS). Tanto la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD), en su disposición adicional primera como el nuevo Real Decreto 311/2022 del ENS así lo exigen.

Las administraciones públicas tienen la obligación de exigir el cumplimiento del ENS para la provisión del producto o servicio objeto de la licitación. Aunque específicamente no lo mencionen, estaremos obligados a su cumplimiento.

¿Qué medidas debo tomar para tratar de evitar ataques?

Desde dar formación a los empleados, hasta implementar medidas técnicas de protección e incluso monitorizar ciertos elementos como la red, incluyendo los puntos de entrada, las aplicaciones y la información. Si no tienes especialistas en tu empresa, contrata a un tercero asesoramiento y trabajos en esta materia.

¿Cuáles son los factores con más peso que van a determinar el sistema de gestión de la seguridad que necesito?

Lo importante es que la gestión de seguridad hay que separarla en dominios para poder gestionarla. Por ejemplo, uno de los más importantes es la protección de los datos, sobre todo datos bajo la regulación de datos de carácter personal (RGPD / LOPDyGDD) y de aquella información empresarial que no debe ser conocida por terceros no autorizados (datos de clientes, oportunidades de negocio, datos de empleados, entre otros).

Adicionalmente el volumen de nuestro negocio digital (ingresos, ventas, clientes y proveedores) es un factor determinante en la definición de nuestra estrategia de gestión de seguridad, así como las obligaciones legales tales como el ya citado RGPD o si trabajamos para el sector público, el Esquema Nacional de Seguridad.

¿Cuál es el nivel de inversión adecuado?

El que nos permita mantener el nivel de riesgo aceptado. Como se decía en la cuestión anterior, el análisis de riesgos debe ser el elemento fundamental que guíe las inversiones en seguridad, una vez que la compañía haya decidido su estrategia y apetito por el riesgo. Lo que parece seguro es que en general, las inversiones en ciberseguridad seguirán creciendo entre un 5 y un 10% este año, sobre todo para que las empresas alcancen esa resiliencia de la que tanto se habla y la partida en la que más se invertirá será la de servicios, según Gartner.

Key Risk Indicators u otros indicadores más recomendables.

Está claro que no se puede gestionar lo que no se mide. Los Key Risk Indicators (KRIs) nos dan una información importante, pero creo que aumentan su valor si los vinculamos directamente con los Key Performance Indicators (KPIs), ya que conocer la relación entre el riesgo y el desempeño de negocio es fundamental para una buena gestión del servicio. Por otro lado organizar los KRIs alrededor de métricas provenientes de los controles CIS (controles de seguridad crítica) puede ser un primer paso para conseguir esa buena gestión.

¿Cuáles son las medidas preventivas más eficaces en materia de ciberseguridad?

Las medidas más eficaces pasan necesariamente por el firme, explícito y comunicado compromiso de la alta dirección y el establecimiento de políticas de seguridad y cumplimiento de estándares. Ante la aparición de aspectos como el teletrabajo, la utilización por parte de los trabajadores de equipamiento propio, etc. es claro que los perímetros se han difuminado. Es preciso, pues, que exista una política clara en la organización que permita o deniegue acciones según sean estrictamente necesarias. Por otra parte, la complejidad creciente en los ataques requiere que para hacerles frente todos los elementos de seguridad actúen de forma coordinada y puedan intercambiar información. Y, por último, la concienciación dentro de las empresas sigue siendo un factor importante de prevención.

¿Quién puede ayudarnos ante un ciberataque? ¿Qué organismos se encargan de la ciberdefensa (pública o privada, nacional o global) y pueden prestar su asistencia a las empresas ante un ciberataque?

En primer lugar: nosotros mismos, minimizando las oportunidades de que un ciberataque tenga éxito, con decisiones, responsabilidades y capacidades adecuadas -al menos las básicas-, tal y como hemos ido desgranando en otras respuestas.

En segundo lugar, una vez visto que son insuficientes nuestros medios (propios y/o contratados), solicitando ayudada a los organismos que tengamos identificados, para esta temática, como autoridades de control/supervisión y sus capacidades de respuesta de estas o de otros organismos.

En el ámbito de las administraciones públicas, el COCS (Centro de Operaciones de la Ciberseguridad de la Administración del Estado y Organismos Públicos) se encarga de la protección de estas entidades. Existen organismos, tales como el Instituto Nacional de Ciberseguridad España (INCIBE), que proporcionan ayuda y seguridad a empresas privadas. También existe un Consejo Nacional de Ciberseguridad (CNC), como apoyo al Consejo de Seguridad Nacional (CSN).

¿Existen en el mercado soluciones de seguridad llave en mano para una pyme?

Realmente ya hay servicios para la pyme que ofrecen distintas empresas, especialmente a través de proveedores de servicios de internet (ISP) o proveedores de hosting.

Los fabricantes de tecnología tienen soluciones puntuales, pero que cubren aspectos muy específicos y que resultan técnicamente complicados para la Pymes. Lo ideal es tener un servicio, no un producto de ciberseguridad, que cubra los elementos básicos de protección como pueden ser: antifraude, datos, web y email, que son los principales vectores de ataque en pymes.

Existen numerosas compañías privadas que proporcionan servicios de seguridad a las empresas. ¿Cómo se mide el nivel de madurez en ciberseguridad? ¿Cómo se encuentra nuestro país a nivel de ciberseguridad en las organizaciones?

Hay informes de consultoras que nos pueden ayudar a entender la situación de España en cuanto a la seguridad, utilizando una de las empresas asociadas de AUTELSI, Deloitte[1], nos dice que el 94% de las empresas españolas ha sufrido al menos un incidente grave de seguridad en 2021. Y la media de incidentes ha subido de 1,6 a 2,13 en un año. El efecto de la pandemia y el gran aumento del teletrabajo es una de las causas.

En cuanto a la situación de las empresas en nuestro país, en comparación con otros países, la situación es buena, según un informe de ITU Global Cybersecurity[2], encontrándonos en los primeros puestos.

[1] https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

[2] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5

¿Dónde está el punto de equilibrio entre el desarrollo de negocio y la ciberseguridad?

El punto de equilibrio estará cuando una organización esté suficientemente bien preparada a nivel técnico, humano y empresarial en el momento de hacer frente a una amenaza o un ciberataque. Entendiendo estar preparado como la capacidad de repeler el impacto del incidente, ser capaces de identificar el origen y las consecuencias de este en la propia actividad y procesos empresariales de modo que sea capaz de recuperar la continuidad de las operaciones de negocio en un tiempo razonable y previamente estipulado.

Adicionalmente, otra forma de expresarlo es cuando su riesgo real (residual) sea igual o inferior a su apetito de riesgo (al umbral identificado por la alta dirección).

¿Hasta qué punto se antepone la seguridad al negocio?

En la actualidad es impensable imaginar una empresa que ya no sea tecnológica. A medida que aumente la automatización y digitalización de las empresas por la necesidad constante de aumentar la eficacia y competitividad con menores costes, mayor será su dependencia de la tecnología. Asumiendo el planteamiento anterior, la ciberseguridad debe estar inmersa en la estrategia de negocio, no sólo como un control ante las amenazas sino también cómo garantía de que los impactos y el tiempo de recuperación ante las inevitables amenazas sea el mínimo.

La seguridad como parte del negocio, frente a las ciber amenazas y riesgos tecnológicos, debe ayudar a garantizar las oportunidades y las operaciones empresariales, así como, en el caso de materializarse una amenaza, a minimizar las pérdidas económicas y el impacto reputacional.

¿Cómo justificar las inversiones en ciberseguridad ante el Consejo?

La mejor herramienta para justificar las inversiones y actuaciones en materia de ciberseguridad es el análisis de riesgos, ya que permite presentar una visión de la situación de la compañía y evidenciar las necesidades de inversión mostrando lo que ocurrirá en caso de no llevarlas a cabo. De esta forma el comité de dirección es consciente del impacto que puede tener autorizar o no esas inversiones.

Por supuesto también sirve de ayuda completarlo con informes de mercado sectoriales sobre amenazas y ciberataques.

Finalmente indicar que, según Gartner, en 2025 el 60% de las organizaciones utilizarán las medidas de ciberseguridad como un factor determinante a la hora de elegir con quién realizar negocios. Con esto queda suficiente justificada la inversión en ciberseguridad.

¿Se nota una mayor sensibilidad e implicación en temas de Ciberseguridad en los Directivos de las compañías?

La evolución positiva ha sido constante. Aquellos profesionales que se están dedicando a la ciberseguridad desde los años noventa, comentan como la relevancia de la ciberseguridad ha ido evolucionando de forma pareja al grado de amenazas a las que el uso creciente de la tecnología y al nivel de exigencia legal que resulta del impacto de las anteriores (sobre todo en la sociedad y en la "forma de vida" de esta).

En los últimos seis años se percibe una mayor aceleración en la comprensión de que sin ciberseguridad no hay negocios, ni sociedad tal y como la entendemos. En boca de INCIBE percibimos en ese cambio:

Poco antes de la pandemia comenzamos a recibir solicitudes por parte de directivos y de puestos estratégicos de diversas compañías y diferentes sectores para que desde INCIBE, pudiéramos llevar a cabo colaboraciones relativas a acciones de formación y concienciación. Su preocupación por las cuestiones en torno a la ciberseguridad, y más concretamente en todo lo relativo a las capacidades de sus empleados en este ámbito era patente. A pesar de que no se trataba de una cuestión que sorprendiera, sí que daba la sensación de que existía un nivel de preocupación mayor.

Todo ello se maximizó con la aparición del COVID19 donde se nos pidió llevar a cabo acciones de concienciación específicas para directivos o puestos de responsabilidad. La situación durante la pandemia elevó los niveles de alerta de las organizaciones y generó mayor interés acerca de las amenazas derivadas del teletrabajo o ataques aprovechando el COVID como señuelo, que podrían afectar a las organizaciones y más que nunca, el apoyo de la alta dirección en estas lides era necesario.

Desde entonces, colaboramos con los comités de dirección de empresas de ámbito privado que nos solicitan ayuda para elevar el nivel de ciberseguridad en su organización, con las herramientas disponibles en INCIBE.

Cuando estoy lanzando una nueva iniciativa IT ¿en qué momento del ciclo de vida de su desarrollo debería comunicársela al responsable de Seguridad para aporten su punto de vista y asegurar que la iniciativa es segura además de eficaz y útil?

Debes incluir al responsable de seguridad desde las partes iniciales del ciclo de vida. Las características de seguridad de una iniciativa IT no son separables de otras características de la

misma. La seguridad forma parte del Negocio y por tanto de sus actividades digitales. De hecho, si la seguridad participa en la iniciativa desde el principio, puede facilitar que la seguridad esté integrada con otras características de las aplicaciones, que las decisiones de diseño de la misma también tengan en cuenta los parámetros de seguridad, y permitir que los niveles de seguridad que ofrece puedan evolucionar en función de la propia evolución de la iniciativa. Esta aproximación integra las capacidades de *Security-by-Default* (Seguridad por defecto) *y Security-By-Design* (Seguridad desde el momento mismo del diseño) que serán crecientemente requeridas en los servicios TI.

Es fácil entender el concepto. Es similar a preguntarse Cuándo deben incorporarse las medidas de seguridad en la fabricación de un nuevo coche. Si lo dejas para el final habría que rediseñar el vehículo y costaría más esfuerzo, tiempo y dinero (y ahora ¿dónde meto el airbag?, por ejemplo).

¿Debo enviar a mi departamento de seguridad los registros de actividad de todos mis servicios TI, tanto Cloud como OnPremise (en mis instalaciones)?

Sí, deberíamos asegurar que los mecanismos de monitorización de seguridad IT (generados en todas las máquinas y servicios) estuvieran implantados y para ello se deben recoger, comunicar y tratar los registros que generan. Esto proporciona la base para tener una capacidad mínima de detección y respuesta rápida a incidentes de seguridad, minimizan la extensión e impacto en caso de sufrir un ciberincidente. Además, permite tener un segundo nivel de alerta ante incidencias técnicas, y posibilidades de mejora de cumplimiento legal.

Tengo toda mi infraestructura en la nube, por lo que no debo preocuparme ante un ataque, ya que tengo todo el servicio subcontratado

---

Aunque la información esté en la nube, debemos asegurarnos de que la información esté protegida, ya sea realizando auditorías propias o solicitando al proveedor que me facilite informes de conclusiones sobre auditorías realizadas por terceros. Ten en cuenta que los servicios que has contratado en la nube son para conseguir una determinada funcionalidad, lo que no implica que se haga con seguridad.

¿Cuáles son los pasos a seguir para avanzar de un modelo de Ciberseguridad clásico a un modelo de ciberinmunidad donde en el diseño y el desarrollo de las aplicaciones se realiza teniendo en cuenta la ciberseguridad?

Si nuestra empresa contrata software a medida (específicamente desarrollado para nosotros), un paso importante para avanzar de un modelo clásico de Ciberseguridad es introducir a un grupo/servicio de especialistas en Seguridad en el desarrollo (AppSec) que identifique una metodología, un ciclo seguro de desarrollo y una verificación del código que se esté generando. Este grupo se dedica al desarrollo de software seguro implementando técnicas de encriptación y seguridad. Este grupo se dedica a entrenar y ayudar a desarrolladoras con procesos para que la seguridad sea parte del ciclo de vida del desarrollo de software (SDLC).

Aparte de centrarse en tener desarrolladoras que entiendan como implementar seguridad, se deberían incluir "security checks" en la fase de creación y construcción (build) de software antes de ser instalado en los distintos entornos desarrollo, test y producción. Estos "security checks" estarán orientados a Owasp, calidad de código, vulnerabilidades etc. La implementación de estos nuevos procesos representa una mejora en la calidad de la seguridad de aplicaciones.

¿Cuál es el impacto y relevancia de la ciberseguridad a nivel de conectividad en las arquitecturas multicloud (más de un proveedor de nube)?

Multicloud se ha convertido, más que en un estándar, en una forma habitual de trabajar para muchas compañías con capacidades medias/altas de potencia y adaptabilidad. Proveedores de Cloud luchan por tener los mejores servicios y las compañías se ven atraídos por obtener los mejores servicios que ayuden a incrementar el negocio.

Las razones para un uso multicloud las encontramos en la búsqueda de objetivos tales como: aumentar la disponibilidad, acercar el dato al consumidor de este o balancear cargas de trabajo en busca de menores costes. Estas son algunas de las palancas que justifican el uso de múltiples nubes.

El impacto es alto, pues a los beneficios de esos objetivos y su impacto positivo se suma un impacto negativo que puede poner en riesgo las operaciones y por lo tanto anular completamente el signo positivo. ¿Cómo controlar un entorno tan heterogéneo? Soluciones como EDGE de perímetro o Hubs de comunicaciones y seguridad, en los que establecer servicios de seguridad centrales proveyendo de identidad, acceso y control a los diferentes servicios consumidos en las diferentes nubes, son soluciones que deben ser exploradas por los responsables de las empresas consumidoras del multicloud.

También, la conectividad multicloud se convierte en aspecto relevante de ese "universo" complejo y variopinto. Las compañías optan por VPNs o MPLS o MPLS especificas (Expressroute en Azure o INterconnets en Google) para establecer conexiones con las diferentes Cloud (Azure de Microsoft, AWS de Amazon, Google Cloud, entre otras).

Estas tecnologías en esencia son las mismas que las empresas han usado tradicionalmente en sus centros de datos propios, si bien, también han experimentado una evolución para alcanzar Niveles de Acuerdo de Servicio (SLAs por sus siglas en inglés) más exigentes, así como una mejora en la seguridad. Por ejemplo, el uso de Tecnologías mTLS (Mutual TLS) facilitadas por los servicios Cloud para poder asegurar una mejor conexión entre aplicaciones en diferentes nubes. También APIs que verifiquen la conexiones para asegurarse que son autorizadas a conectarse y otros sistemas de prevención de ataques han añadido a una nueva faceta que mejora, moderniza y agiliza las conexiones de multicloud.

¿Es comparable, en general, la madurez en la ciberseguridad de IT en comparación con la de la OT?

Inicialmente, la forma de entender el uso de la tecnología el mundo de las oficinas y centros de datos, lo que llamamos IT (*information technologies*), era radicalmente diferentes al entorno de fábricas y plantas industriales (lo que llamamos OT (*operation technologies*).

Grosso modo, los sistemas IT se especializaban en la gestión y en la comunicación, mientras que los de OT en la operación en planta. Los primeros con sistemas más abiertos (de multipropósito) y los segundos muy ligados a los sistemas físicos implantados (robots, maquinaria específica, etc..). Incluso los objetivos de la seguridad eran diferentes: en IT que las personas no hicieran daño a las máquinas (y a los datos por ellas manejadas) y en OT que las máquinas no hicieran daño a las personas.

La necesidad de conectar la capa de producción a la capa de decisión (para que tenga mejor información a la hora de tomar decisiones) y a su vez acercar la capa de decisión a la de producción (para una producción más optima, con costes más ajustados), así como el uso de tecnologías de la información del mundo IT en el OT (redes ethernet, sistemas unix, wifis, el telemantenimiento, entre el largo etc), no sólo han acortado sus diferencias sino que anticipan un mundo de convergencia que en nada de tiempo proveerá de un único espacio común al IT y al OT.

Aunque se está avanzando rápidamente para que exista una convergencia entre ambos entornos, lo cierto es que en materia de ciberseguridad en el caso de las OT aún queda camino por recorrer. Uno de los principales escollos a superar, es que las tecnologías empleadas en los entornos de la operación no suelen, o solían ser conocidas por los técnicos del ámbito de IT, en parte debido a que ambos entornos eran operados por perfiles diferenciados. Mientras que el ámbito OT era gestionado por ingenieros y operadores, los sistemas informáticos convencionales eran administrados por técnicos de IT añadiendo además, que la interconexión entre ambos "mundos" era muy limitada impidiendo que las arquitecturas de los entornos de la operación se pudieran beneficiar de las características de ciberseguridad existentes en el ámbito TI. Otro inconveniente, es la existencia de tecnologías y protocolos de comunicaciones que, por su antigüedad entre otras cosas, no se encuentran alineados con las directrices mínimas de seguridad que se requieren en la actualidad, aunque actualmente existen soluciones que permiten mejorar sus características en este campo.

Afortunadamente y desde hace unos años este escenario ha cambiado y se está avanzando hacia un contexto de convergencia entre las IT y las OT, por los beneficios que esto supone respecto al aumento de los dispositivos de campo y soluciones inteligentes que se conectan a Internet, el incremento de las comunicaciones y la necesidad de reducir el riesgo o las amenazas de ciberseguridad en las tecnologías de la operación. Pero sin duda y sobre todo, para conseguirlo será necesario que los equipos de IT y OT trabajen de forma conjunta.

¿Creéis que otras tecnologías como la inteligencia artificial pueden mejorar los niveles de detección y defensa en materia de ciberseguridad?

Sin duda una de las características que tiene la inteligencia artificial (IA) es su capacidad de aprendizaje automático de manera independiente en base a patrones establecidos con un propósito concreto. Si trasladamos este objetivo a algún campo de la ciberseguridad (como por ejemplo la detección de malware), estaremos ante una solución que, además de reaccionar de manera más rápida y más precisa, irá aprendiendo con el paso del tiempo de tal manera que sea capaz de tomar decisiones y predecir posibles evoluciones del problema.

No obstante, hay que señalar que la evolución de la IA en el ámbito de la ciberseguridad no se encuentra tan avanzado como en otros. En la actualidad las soluciones basadas en "*machine learning*" se centran en el análisis de gran cantidad de datos para determinar la probabilidad de ocurrencia de un tipo de evento, lo que se denomina el pronóstico predictivo. Por lo tanto, servirán para analizar situaciones de riesgo y la detección de anomalías en el lado preventivo; y mejorar la resiliencia, adaptabilidad y flexibilidad en el lado reactivo.

No obstante, es importante señalar que esta tecnología, del mismo modo que ayuda en procesos de detección, por ejemplo, también podría ser utilizada para diseñar procesos de evasión y que las amenazas fueran más difíciles de detectar.

Para entender mejor la necesidad que subyace a la pregunta, pensemos que un único sistema de información, en su uso diario, puede generar entre mil y cien mil eventos de seguridad (informaciones de uso que aportan conocimiento a la seguridad). La necesidad de tratar la ingente información que los sistemas generan, así como la de analizarla, evaluarla y tomar rápidas decisiones harán de la aplicación de la inteligencia artificial y de la mecanización de acciones de respuesta, dos potentes armas de ciberdefensa.

Agradecimientos

Desde AUTELSI agradecemos la colaboración en la formulación de las preguntas a los siguientes responsables de sistemas de información, de algunas de las principales empresas del país:

Nicolás Elías Vinuesa es ingeniero industrial por la Universidad Politécnica de Madrid y PDD por el IESE. En 2006 pasó a ser el CIO de Enagás. Entre sus responsabilidades se encontraban las comunicaciones y la Ciberseguridad tanto en el ámbito IT como OT, participando en la transformación digital de la empresa. Su carrera profesional comenzó en el Grupo Alcatel, donde trabajó en la división de consultoría y formación en diferentes puestos. En el año 2000 se incorporó a Telefónica Data Corporation como Gerente de Procesos de Negocio. En esa posición, definió e implementó el modelo de proceso de negocio de la compañía en ocho países. En 2002 asumió el cargo de CIO en Telefónica International Wholesale Services, que en ese momento tenía oficinas en más de diez países. Además de la IT interna, fue responsable del desarrollo de aplicaciones para clientes. Miembro de la Junta Directiva de AUTELSI.

Juan Manuel García García, es Ingeniero Informático. Durante su primera etapa profesional se especializó en la consultoría técnica de sistemas y trabajó en el ámbito de la consultoría donde ocupó diferentes puestos de responsabilidad. Desde su llegada a Repsol en el año 2006 ha asumido varias responsabilidades, inicialmente en el área de la Dirección de Desarrollo y Arquitectura, para posteriormente moverse a la dirección de Sistemas de Exploración y Producción, de la cual se hizo cargo como máximo responsable el año 2018. Desde septiembre de 2022 Juan Manuel es el CIO&CDO de Repsol dentro de la Dirección General de Transición Energética, Tecnología, Institucional y Adjunta al CEO. Anteriormente ocupaba el cargo de director de Servicios IT & Digital. Miembro de la Junta Directiva de AUTELSI.

Víctor Moro Gil, ha estado 40 años en el mundo de los seguros ligado a la TI, ha desarrollado su carrera en compañías como Winterthur o Liberty en Portugal y, desde el año 2004 en Mapfre donde era el director de Tecnología de Iberia (España y Portugal) CIO MAPFRE ESPAÑA. En su formación cuenta con un Máster en Sistemas y Tecnologías de la Información por Ide-Cesem. Miembro de la Junta Directiva de AUTELSI.

José Valdelvira Jiménez, Licenciado en Ciencias Matemáticas, Estadística e Investigación Operativa por la Universidad de Granada y PDD por el IESE, ha desarrollado la mayor parte de su actividad profesional en CLH, actualmente grupo Exolum, empresa líder en España en el transporte y almacenamiento de productos petrolíferos y una de las mayores empresas privadas de su sector a nivel internacional. Vinculado siempre a la Dirección de Sistemas de Información desde 1989, ha ocupado diferentes puestos de responsabilidad y ha liderado proyectos importantes que han contribuido a la transformación de los sistemas de la compañía.. Desde el 2010, como director de Sistemas de Información, lidera el área de IT y OT en Exolum, asumiendo el reto de la internacionalización de la compañía y la evolución tecnológica de la misma. Miembro de la Junta Directiva de AUTELSI.

Carlos Varela Ávila, Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid. Desde 2014 es director de Transformación Digital y Tecnología en la Dirección General de Estrategia y Desarrollo de Renfe Operadora. Anteriormente desempeñó distintos cargos en la organización IT de Renfe donde ha trabajado desde 1989, entre otros: director de producción, Director de Ingeniería de sistemas y comunicaciones, Jefe de Técnica de sistemas y Jefe de Administración de bases de datos. También en el sector de los sistemas de información ha trabajado en Serbal informática Avanzada, Computing Technology Consulting (CTC) y Rank Xerox España. Miembro de la Junta Directiva y Presidente del Grupo de Telecomunicaciones de AUTELSI.

Susana Zumel Vara, Ingeniera Industrial que ha desarrollado su carrera profesional en el ámbito de la tecnología, trabajando para diferentes consultoras (IBM, EY, Deloitte) con una especialización en el sector energético. En 2004 se incorporó al equipo de Sistemas de Información de Cepsa, donde ha desempeñado diferentes funciones (Desarrollo y Mantenimiento de Aplicaciones, Gobierno y Arquitectura de TI, Estrategia de TI) hasta que pasó a ocupar la posición de CIO en el año 2018. Miembro de la Junta Directiva de AUTELSI.

Asimismo, agradecemos de forma expresa el trabajo realizado por los profesionales expertos en seguridad que han participado en la formulación de las respuestas recogidas en el cuestionario, miembros del Grupo de Seguridad de AUTELSI:

Francisco Lázaro Anguís, es Gerente de Ciberseguridad y Privacidad del Grupo Renfe. CISO de Renfe, Delegado de Protección de Datos de Renfe, Profesor Asociado de la ETSI de Telecomunicaciones de la UPM, Cruz con distintivo blanco de la orden del mérito de la Guardia Civil. Presidente del Grupo de Seguridad de AUTELSI.

Javier Asenjo Muñiz, director de RRHH y consultor de RRHH. Master en RRHH, PRL y SCRUM Master. Ha desarrollado tu trayectoria profesional en importantes compañías tecnológicas multinacionales. Actualmente lidera la función de RRHH NCR en Iberia. Miembro del Grupo de Seguridad de AUTELSI.

Mariano J. Benito Gómez, es CISO desde 2004, junto con otras responsabilidades en Continuidad de Negocio, Privacidad, Cumplimiento Legal y Cloud Computing. Está certificado CISA, CISM, CGEIT, CDPSE y CRISC; CISSP; CDPD, DPO y CDPP; ISO 27001-LA, BS 25999-LA. Implementó en 2004 y opera desde entonces un SGSI basado en ISO 27001 (Certificación más veterana en vigor). En 2010 implantó un SGCN basado en ISO 22301 (2a certificación en España), y en 2019 un SGIP basado en ISO 27701. Participa regularmente en medios de comunicación y congresos del sector. Miembro del Grupo de Seguridad de AUTELSI,

Javier García-Romanillos Henríquez de Luna, Responsable de políticas de ciberseguridad y de formación y concienciación del Grupo IAG – International Airlines Group (Aer Lingus, British Airways, Iberia, Iberia Express, Vueling, etc.). Con más de quince años de experiencia en el ámbito de la seguridad de la información, ha desarrollado gran parte de su carrera profesional como consultor y auditor de riesgos y tecnologías de la información en EY. Es Ingeniero Técnico Informático (UPSAM) y posee las certificaciones CISA, CISM y CRISC por ISACA; Lead Auditor ISO 27001 por BSI; Lead Auditor ISO 22301 por Tüv Nord; Experto Técnico por EuroPriSe; ITIL v3. Miembro del Grupo de Seguridad de AUTELSI.

María Ángeles Gutiérrez Puente, ha desarrollado su carrera profesional en distintas multinacionales siempre en el sector de la ciberseguridad tanto en el ámbito de la tecnología como en el de riesgos y regulatorio. Es Licenciada en Física y Master en Inteligencia. Actualmente lidera el equipo de GRC en NTT Data. Miembro del Grupo de Seguridad de AUTELSI.

Javier Jiménez Pajares, Ingeniero Industrial por la Universidad Politécnica de Madrid y master por el IESE, ha desarrollado la mayor parte de su carrera profesional en Extreme Networks, fabricante de equipamiento y soluciones de comunicaciones y seguridad, ocupando diferentes puestos nacionales e internacionales, siendo actualmente director general de la compañía para España. Miembro de la Junta Directiva y del Grupo de Seguridad de AUTELSI.

Marco Antonio Lozano Merino, Ingeniero de software y Diplomado en tecnologías de la Informática por la Universidad SEK, Marco A. cuenta con una amplia carrera en el área de la ciberseguridad desempeñando tareas como asesor y consultor tecnológico desde hace más de 19 años en empresas de diversos ámbitos que discurren desde los medios de prensa hasta la Administración Pública. En la actualidad ejerce como responsable de Servicios de Ciberseguridad para Empresas en el Instituto Nacional de Ciberseguridad (INCIBE), forma en diversos másteres de ciberseguridad y colabora con la Comisión Europea y diversos medios de comunicación. Cuenta con una amplia formación y certificaciones como CISM, GIAC, CCS-G, CCS-T, ITIL e ISO 27000 entre otras. Miembro del Grupo de Seguridad de AUTELSI.

Iciar Alonso Ollacarizqueta, Ingeniera Industrial. Jefa de Servicio de Nuevas Tecnologías y Sociedad de la Información del Gobierno de Aragón desde 2004. Ha participado en la elaboración de diversos planes estratégicos como los Planes directores de la Sociedad de la Información en Aragón y la Estrategia Aragonesa de Open Data. Como jefa de servicio es responsable del proyecto de apertura de datos del Gobierno de Aragón y del portal de Servicios del Gobierno de Aragón. Miembro del Grupo de Seguridad de AUTELSI.

Ramón Ortiz Gonzalez, Ingeniero Técnico Informática Gestión; CISA, CISM por ISACA; PA Compliance en el IE Certified Cyber Security Professional por ISMS Forum Spain y Master en Dirección de eCommerce y Marketing Digital por FED Ha desempeñado cometidos en diferentes empresas como Tragsa, en proyectos de control por teledetección, proyectos de banca a distancia en diferentes entidades (Caja Ahorros de Navarra, Argentaria, SolBank-Sabadell) y en proyectos para la Administración Pública. En 2001 comenzó a trabajar en Mediaset España primero en el Área de Organización y Procesos y, posteriormente en el Departamento de Desarrollo Estrategico de la División Publicitaria de la Compañía. Desde 2006 es el responsable de Seguridad de Mediaset, con responsabilidad sobre la Ciberseguridad de los Sistemas IT y Broadcast, y es miembro de la Unidad Corporativa de Mediaset de Privacidad de los Datos, entre otros cometidos. Adicionalmente colabora en desarrollar e impartir sesiones de concienciación sobre Ciberseguridad y Privacidad a los empleados de las empresas del grupo Mediaset España. Es miembro de grupos de trabajo en ISMS Forum, AUTELSI y del Foro Nacional de Ciberseguridad del DSN y colaboro habitualmente como ponente en foros sectoriales de Ciberseguridad.

Pablo Pérez San-José, es Senior Manager de Ciberseguridad en Deloitte, donde dirige y participa en proyectos de asesoramiento en la estrategia y mejora de las cibercapacidades de las organizaciones y de servicios gestionados de operación y respuesta a incidentes. Profesor asociado de Máster de la Univ. Carlos III y de la Escuela Internacional de Postgrado (EIP). Coautor y colaborador de estudios e investigaciones en materia de seguridad, privacidad y confianza digital para, entre otros, el BBVA Global Observatory, el Observatorio de la Seguridad de la Información de INTECO, el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) o el Grupo de Análisis y Prospectiva de las Telecomunicaciones (GAPTEL). Miembro del Grupo de Seguridad de AUTELSI.

Juan Miguel Velasco López-Urda es actualmente CEO y Fundador de AIUKEN CYBERSECURITY, multinacional española especializada en Ciberseguridad, Internet y Servicios Cloud de Ciberseguridad, que opera en 7 países (España, Portugal, Chile, Emiratos, Marruecos, Arabia Saudi y Costa de Marfil), además es consejero de varias compañías de Seguridad Internet, profesor asociado del Instituto de Empresa y secretario del Consejo Asesor de ISMS Forum Spain. Cuenta con más de 20 años de experiencia en Telecomunicaciones, Tecnologías de Información y Seguridad y ha desempeñado distintos cargos directivos en Grandes Compañías líderes en el sector de Seguridad y Telecomunicaciones como Telefónica Empresas, Telefónica Data, Agencia de Certificación Electrónica y Alcatel. Miembro del Grupo de Seguridad de AUTELSI.

Desde la Asociación queremos agradecer la colaboración de las entidades que hicieron posible la presentación de este trabajo, en el evento celebrado el 18 de abril de 2023:

Agradecemos el apoyo institucional de **INCIBE**, el patrocinio de **AIUKEN, GMV** y **TELEFÓNICA** y la colaboración de **CEPSA,** el **GOBIERNO DE ARAGÓN** y **RENFE**. Estas entidades y las personas que las representaban hicieron posible la presentación de este trabajo, en el Seminario que se celebró el 18 de abril del 2023 en el Hotel Bless de Madrid.