DOCUMENTOS
SiC
Nº 20
FEBRERO 2016

accenture

Ciberseguridad: dimensión global e innovación al servicio de la era digital

ENTREVISTA

David Pérez Lázaro

Managing Director, Responsable de Negocio de Seguridad para España, Portugal e Israel

TRANSFORMACIÓN DIGITAL
Servicios globales de seguridad inteligente

ANÁLISIS DE MERCADO
Tendencias para la protección empresarial

La compañía hace de la seguridad una prioridad para la transformación digital de las empresas

Accenture presta servicios globales de Seguridad Inteligente

Accenture ha situado a la ciberseguridad en el primer plano empresarial, como elemento clave para la Transformación Digital del negocio, la resiliencia de la infraestructura y la protección de los activos críticos para la actividad de las organizaciones. La compañía está enfocada en el crecimiento estratégico de esta área, para la que ha construido un sólido catálogo de servicios capaces de responder a las necesidades de cualquier organización.

"*Debemos acompañar a nuestros clientes e involucrarles en conversaciones sobre la seguridad de sus organizaciones. Una estrategia de seguridad y un enfoque en ciberdefensa adecuados en el core del negocio son claves para su resiliencia y la confianza en la marca. La seguridad es un área de crecimiento estratégico para Accenture, así como una prioridad para mí y mi equipo de liderazgo*". Con estas palabras, **Pierre Nanterme**, CEO y Chairman de **Accenture**, dejaba claro el foco que la compañía está haciendo en la seguridad, un elemento clave para la transformación digital de las empresas.

La visión de Accenture se basa en la imbricación de dicha seguridad en los procesos de negocio de las empresas. Para ello ofrece soluciones de Seguridad Inteligente escalables y a medida con las que garantizar el camino hacia la innovación y el crecimiento de cada cliente. Tanto es así, que la compañía ha dado un paso significativo al incorporar su compromiso con la seguridad de la información y la privacidad de los datos a su Informe de Responsabilidad Empresarial.

Entender el mercado

Accenture ha construido una oferta de servicios a partir de una comprensión nítida de lo que está ocurriendo en el mercado empresarial y cómo la ciberseguridad se ha convertido en un eslabón clave para la supervivencia y el devenir de cada organización.

La actualidad está marcada por la falta de un alineamiento efectivo entre los objetivos comerciales de las empresas y sus programas de seguridad, ya sea por la escasez de personal preparado, ya sea por la falta de comprensión de los aspectos más técnicos. A esto se une el hecho de que muchas organizaciones consideran cubierto el apartado de seguridad limitándose a cumplir con la normativa y las regulaciones vigentes.

Asimismo, los límites de las estructuras empresariales se han difuminado con los modelos de pago por uso y la movilidad de sus trabajadores. Esto ha disparado, aún más, las amenazas a las que se ven expuestas, las cuales, desafortunadamente, han pasado a ser más persistentes y complicadas de identificar.

ASOC (Accenture Security Operations Center) en España.

Accenture comprende y afronta este escenario y enfoca su oferta de servicios al desarrollo de plataformas de seguridad inteligentes alineadas con la estrategia de cada negocio.

Para lograr el objetivo de establecer inteligencia de seguridad en la empresa digital, la compañía apuntala su trabajo con los clientes proponiendo cinco pasos: la evaluación de la capacidad del programa de seguridad y la identificación de oportunidades; la gestión de la complejidad y su integración en la

El compromiso con la ciberseguridad, objetivo prioritario en la Responsabilidad Social Corporativa de Accenture

Accenture España ha dado un paso significativo en la prioridad de la ciberseguridad al incluirla como un punto clave en su "Informe de responsabilidad empresarial". Esta decisión resulta, sin duda, diferencial en el mercado y pone en primera línea de acción el compromiso que la compañía asume en la protección de sus clientes.

"La unión de la Responsabilidad Social y la Seguridad, a partir de un trabajo conjunto, tiene como objetivo mejorar la sostenibilidad de la compañía", asegura David Pérez-Lázaro, Managing Director y Responsable de Negocio de Seguridad para España, Portugal e Israel de Accenture.

Concretamente, la compañía se compromete con sus clientes a la "Seguridad de la Información y la Privacidad de los Datos". Para ello, Accenture hace gala de la certificación ISO 27001 tanto del Spain Delivery Center y como para Iberia GU (España, Portugal e Israel) dentro de su programa de certificación global.

A esto añade responsabilidad sobre la protección de los datos del cliente, sobre el empleo de las mejores tecnologías para llevar a cabo tal cometido, y sobre su capacidad de formación y comunicación, con casi 8.700 horas de formación en relación con la privacidad de los datos y la seguridad de la información.

Asimismo, Accenture ha construido exhaustivas políticas internas con relación a la privacidad, al procesamiento de los datos personales y a los derechos de los individuos sobre los datos gestionados de la compañía, ha creado la figura del Data Privacy Officer y pone a disposición de las empresas su Accenture Security Operations Center (ASOC).

empresa; la mejora de la agilidad en estos procesos; la aceleración definitiva a la citada Seguridad Inteligente; y finalmente, el desarrollo de estrategias operativas flexibles.

Catálogo de servicios

Esta estrategia de Accenture se traduce en un catálogo de servicios *end-to-end* específicos para cada industria y cimentados en la labor de una amplia terna de especialistas, así como en las tecnologías de fabricantes contrastados. La oferta se divide en cuatro áreas (ver **Figura 1**):

- **Evaluación y Arquitectura**. Servicios profesionales de análisis y asesoramiento sobre las capacidades actuales y el modelo operativo de gestión de la seguridad, así como de la identificación y gestión del ciclo de vida de las amenazas y los riesgos, apoyándose en marcos metodológicos propios y herramientas de referencia en el mercado.
- **Identidad Digital**. Accenture se adelanta a una de las principales necesidades del mercado con servicios enfocados en la gestión de las identidades y accesos tanto a nivel de usuarios empresariales, como de clientes (B2C) y cosas (IoT).
- **Ciberdefensa**. Área en pleno desarrollo, especialmente tras a la adquisición de la compañía FusionX. En ella, Accenture proporciona servicios de inteligencia, analíticas avanzadas o monitorización de operaciones, entre otras capacidades.
- **Servicios de seguridad gestionada**. Servicios gestionados seguridad avanzada (ciberdefensa, identidad, cumplimiento, entre otros), respondiendo a una doble problemática: la dificultad para los clientes de contratar y retener a personal experimentado en las últimas tendencias, y la puesta en marcha de modelos operativos que permitan afrontar los nuevos retos. Se trata de servicios elásticos, adaptables a las necesidades cambiantes incluso a nivel global, tanto en modo *standalone* como formando parte de grandes contratos de infraestructura.

Este catálogo de servicios toma en consideración la aparición de tecnologías emergentes en torno a la seguridad *cloud*, móvil y del Internet de las Cosas (IoT), en cuya investigación Accenture está invirtiendo de manera decidida para seguir adelantándose a las necesidades de sus clientes.

Actor destacado en ciberseguridad

La prioridad que Accenture confiere a la ciberseguridad, plasmada en su catálogo de servicios y soluciones, se traduce en una propuesta de valor para fidelizar a sus clientes: ayudarles a fomentar la confianza en sus negocios, a menudo en plena transformación digital (en la actualidad ya trabajan en optimizar la seguridad de más de 300 clientes). De hecho, el objetivo que la consultora se ha marcado pasa por convertirse en un actor clave para aquellas empresas que deseen acercar la función de seguridad al nivel ejecutivo del negocio, de manera que la seguridad siempre esté alineada con los objetivos estratégicos del negocio mediante una efectiva arquitectura de seguridad empresarial. En ese camino están apostando por un crecimiento exponencial, tanto en recursos como en alianzas tecnológicas, de tal modo que el cliente tenga a su disposición los más amplios conocimientos y experiencia, combinados con las tecnologías y prácticas más innovadoras del mercado.

Figura 1

Otros puntos primordiales en la concepción de la apuesta por la ciberseguridad que Accenture está realizando son una continua inversión en I+D, para ofrecer mayores capacidades en los ámbitos de la inteligencia de seguridad, sistemas adaptativos y modelos operativos que ayuden a sus clientes a alcanzar el equilibrio entre una superficie de riesgo que no para de crecer (con aspectos como el *cloud*, la movilidad o la explosión de tecnologías, dispositivos, canales y usuarios) y la seguridad como una prioridad en la agenda de los equipos ejecutivos (con crecientes riesgos operacionales, reputacionales y legales).

Asimismo, la filosofía de Accenture incide en mejorar la resiliencia del negocio de sus clientes, aportándoles capacidades de ciberdefensa de próxima generación, con las que se encuentren en disposición de afrontar el ciclo de vida de la seguridad al completo: desde la identificación, hasta la recuperación frente a los ataques, pasando, por supuesto, por la protección, detección y respuesta. En este sentido Accenture pone a disposición de sus clientes los Accenture Security Labs, un centro de investigación donde conectarles con su red de expertos y conocimiento a nivel mundial.

Clientes: tipología

Esta visión de la ciberseguridad está teniendo un gran calado en importantes clientes, especialmente en los sectores de Banca y *Resources*, en los cuales Accenture ha puesto en marcha proyectos de toda índole: desde la migración de la gestión de identidades y accesos para los 350.000 usuarios globales de una operadora, hasta la remediación de problemas de seguridad a todos los niveles en uno de los principales bancos de la región Asia/Pacífico, pasando por sendos proyectos en compañías del sector petrolífero/gas, en los que se ha optimizado la gestión de riesgos, ha multiplicado la ciberseguridad y ha potenciado el control de las redes. ●

David Pérez Lázaro Managing Director, Responsable de Negocio de Seguridad para España, Portugal e Israel

Accenture es una compañía global de servicios que ha situado hoy a la ciberseguridad como una de sus principales líneas estratégicas. En la presente entrevista, David Pérez Lázaro, Managing Director, Responsable de Negocio de Seguridad para España, Portugal e Israel, explica el plan de transformación y ampliación de capacidades de su compañía en este segmento de mercado, en cuyo marco juega un papel muy significativo su estructura en Iberia.

"Accenture apuesta por la definición de una Arquitectura Empresarial de Ciberseguridad integrada con la transformación digital de los negocios"

– ¿Conoce usted a muchas multinacionales de origen español que hayan incluido de modo explícito en su informe de Responsabilidad Social Corporativa la gestión de la seguridad de la información y el respeto por el principio de privacidad?

– Aunque la ciberseguridad ya ha llegado a la agenda de los Comités de Dirección de las grandes empresas, fundamentalmente debido al incremento de la presión normativa y los cambios legislativos recientes, todavía no se ha instalado en el ADN de las compañías hasta el punto de formar parte del núcleo de su responsabilidad empresarial.

Accenture en España ha sido pionera incluyendo la seguridad de la información y la privacidad de los datos como una máxima que aplica en todos sus procesos y servicios a lo largo de nuestra cadena de valor, dentro de nuestro Informe de Responsabilidad Empresarial, sometido además a una revisión por un proveedor externo independiente de acuerdo con el estándar internacional ISAE 3000.

– ¿Cuáles son los aspectos diferenciales de Accenture en lo que afecta a la provisión de servicios de ciberseguridad?

– En primer lugar, somos una empresa global, lo que es clave para dar respuesta a las amenazas de ciberseguridad en un contexto donde la captación de talento es un reto tanto para nuestros clientes como para las empresas de servicios como nosotros.

En segundo lugar, somos una compañía eminentemente tecnológica, con alianzas con los principales proveedores de ciberseguridad del mercado y capacidades de *delivery* industrializado a través de nuestros centros.

Finalmente, contamos con centros de Innovación específicos en ciberseguridad donde se han integrado tecnologías novedosas en ámbitos como *analytics*, automatización y orquestación de procesos, etc., que ahora forman parte de nuestra oferta diferencial de servicios.

– ¿Cuántas personas trabajan en Accenture a escala global en las distintas líneas de oferta de servicios de ciberseguridad, y cómo está organizada la Corporación en esta línea de mercado?

– Somos más de 2.300 profesionales dedicados a ciberseguridad a nivel global y aspiramos a superar los 3.000 antes de finales de agosto de 2016. Nuestra organización se divide en áreas geográficas, donde España lidera una de ellas denominada Iberia, que incluye a Portugal e Israel. Cada geografía distribuye sus recursos en 3 grandes áreas: Transformación (el área tradicional de *consulting*), Implementación (especializada en despliegue de tecnologías) y Servicios Gestionados.

– Accenture adquirió hace meses la compañía FusionX, especializada en simulación de ataques y modelización de ciberamenazas sofisticadas. ¿Tienen previsto realizar otras adquisiciones en otros frentes del mercado de ciberseguridad?

– Sí, FusionX fue la primera adquisición realizada dentro de un plan de crecimiento inorgánico más amplio. Recientemente se ha anunciado también la compra de Cimation, una compañía de consultoría especializada en "Industrial Internet of Things" (IIOT) con un área específica de ciberseguridad para los entornos de control industrial.

Este plan de crecimiento inorgánico se va a extender a Europa en este año. El hecho de que Israel forme parte del ámbito geográfico bajo mi responsabilidad nos va a dar un papel muy relevante en el desarrollo de esta estrategia, que aportará capacidades diferenciales para nuestros clientes en España.

– Accenture dispone del ASOC (Accenture Security Operations Center). ¿Qué inversiones tiene previsto acometer para constituir una red de centros acorde con el plan estratégico del Grupo?

– Un elemento clave es la ampliación de nuestras capacidades en Europa. Para ello nos apoyaremos en los centros ya existentes –fundamentalmente en Praga y Madrid– y los integraremos con las capacidades avanzadas de ciberseguridad derivadas de nuestra estrategia de expansión en Israel.

De forma práctica nuestro "Iberia Cyber Hub" integrará las capacidades existentes en España de consultoría, implantación y servicios gestionados con nuevas capacidades avanzadas en ciberseguridad desde Israel. La primera línea de servicio de este centro orientada a la prestación de servicios "GRC as a Service" ya está en marcha gracias a la experiencia adquirida en España en los últimos años

"Estamos ampliando capacidades de MSSP en Europa, apoyándonos en los Accenture SOC existentes –principalmente en Praga y Madrid–. Dichas capacidades se consolidarán en nuestro Iberia Cyber Hub, en el que también integramos las capacidades avanzadas de ciberseguridad derivadas de nuestra estrategia de expansión en Israel".

– Vivimos tiempos de transformación digital. ¿En qué sectores de la economía se ubican las empresas que se han quedado retrasadas en lo que toca al grado de madurez en la integración de la ciberseguridad en los procesos de negocio?

– La verdadera transformación digital está todavía por llegar. Hasta ahora las empresas han dado "pequeños pasos" digitales, donde por cierto la seguridad no ha sido en su mayoría un elemento ni mucho menos clave o se ha quedado en una declaración de intenciones en papel.

En ciberseguridad una verdadera transformación digital tiene implicaciones diferenciales en aspectos como la gestión de la identidad digital de clientes, la protección de activos críticos y la capacidad de predecir las amenazas y tener capacidad de respuesta en tiempo real.

Aquellos sectores donde la seguridad de la información ha sido clave para el negocio, fundamentalmente el financiero, se encuentran mejor preparados y ya están dando el salto digital con "red de protección". En el resto, donde la madurez de la función de seguridad ha sido tradicionalmente inferior (por supuesto con honrosas excepciones) se pueden producir saltos digitales "al vacío", con el "ciberriesgo" que eso conlleva.

– Si tuviera que citar tres líneas de proyectos de ciberseguridad por acometer que a fecha de hoy considera usted que son una asignatura pendiente para la mayoría de compañías usuarias, ¿cuáles serían?

– Por serle sucinto: Planes de Ciberseguridad Globales, orientados de forma práctica a evaluar las amenazas y mitigar el impacto de los riesgos de ciberseguridad en el negocio mediante enfoques basados en Inteligencia de amenazas que difieren en 180º de los planes directores de seguridad tradicionales; Implementación de Procesos de Respuesta y Defensa Activa, no sólo de detección como se ha hecho principalmente en los últimos años, empezando a incluir procesos de orquestación y respuesta automáticos; y Analytics, o como empezar a aplicar tecnologías analíticas a casos de uso específicos (p.ej análisis de comportamiento)

– ¿Hay una manera realista de imbricar la ciberseguridad con el negocio?

– Creo que sí, y en este punto, compañías como Accenture, que estamos liderando la transformación digital de nuestros clientes, tenemos mucho que decir. Nosotros desde el área de Seguridad estamos trabajando de forma integrada con los distintos verticales de negocio y nuestras áreas especializadas en Estrategia y Digital para llevar este mensaje a nuestros clientes mediante la definición de la Arquitectura Empresarial de Seguridad.

Para ello estamos siendo pioneros en España en formar y certificar a nuestros profesionales en SABSA, la metodología que entendemos es la más adecuada para seguir un enfoque holístico y probado en grandes organizaciones para conseguirlo.

Obviamente este es un esfuerzo que debe ser liderado desde la Dirección e integrado en los procesos de transformación *top-down*. Realmente creemos que quien sea capaz de integrar la ciberseguridad en sus procesos va a tener una ventaja competitiva muy importante y no tardaremos en verlo en aquellos clientes que adopten este enfoque. ●

Accenture analiza las tendencias para la mejora de la protección empresarial

El futuro de las empresas depende de la integración de la ciberseguridad en los procesos de negocio

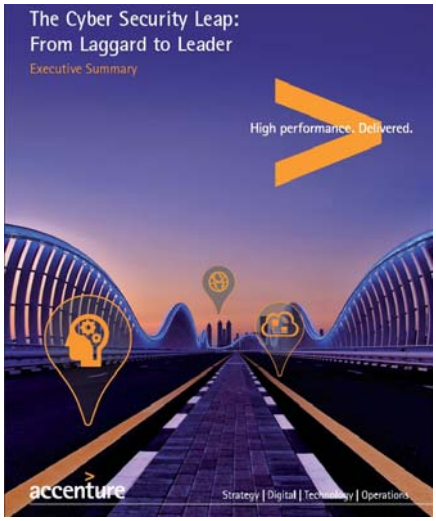
La movilidad, el Internet de las Cosas (IoT), el incremento de las cargas regulatorias y el almacenamiento y procesamiento masivo de datos, en algunos casos deslocalizado, están cambiando las necesidades de las empresas que han de plantearse la ciberseguridad como un activo esencial para su supervivencia y desarrollo. Accenture trabaja con sus clientes en ese sentido para analizar lo que está por venir en un futuro próximo.

La genética evolutiva de una compañía como **Accenture**, capaz de sondear el mercado empresarial para definir qué demanda y demandará a corto, medio y largo plazo, es uno de los valores diferenciales que ofrece a sus clientes. No en vano, su amplio catálogo de servicios se fundamenta en esta capacidad de análisis, la cual refleja en los distintos estudios e informes que publica.

"The Cyber Security Leap" es el título del estudio que ha llevado a cabo junto al **Instituto Ponemon**, en el cual, ambas entidades exploran los factores de éxito de una serie de empresas que durante un periodo de dos años mejoraron su efectividad en el ámbito de la ciberseguridad. En este ejercicio, constataron que las empresas que dan el salto a un mayor nivel de eficiencia en la seguridad (un 53% de mejora promedio) consiguen una efectividad superior mediante tres áreas clave: estrategia, tecnología y gobierno, con respecto a las que permanecen estáticas (que mejoran un 2% promedio). (Ver **Tabla 1**)

Accenture ofrece una guía a aquellas empresas que desean recorrer el camino de la evolución en sus procesos de seguridad hasta convertirlos en críticos para el negocio.

Profundizando en las diferentes perspectivas de la seguridad entre las empresas con una concepción estática y las que buscan una correcta evolución, el estudio de Accenture y Ponemon apunta que la estrategia que han seguido estas últimas ha pasado por otorgarle un rol más decisivo al CISO y por dedicar un mayor presupuesto a la seguridad, lo que ha redundado en contar con un mayor equipo destinado no solo a la prevención sino también a la detección de amenazas,



frente a las estáticas, que dedican un menor presupuesto y que suelen limitarse a la prevención de amenazas.

No en vano, las compañías que mejor se han adaptado le otorgan una mayor importancia a la seguridad de la información como prioridad del negocio, y esto les lleva a alinearla con los objetivos estratégicos. Asimismo, esta visión les prepara mejor para afrontar las distintas vicisitudes a las que se ven sometidas. Un buen ejemplo son los ataques persistentes, a cuyos riesgos se adaptan más rápidamente, de modo que responden mucho antes que las organizaciones estáticas, las cuales también tienen un déficit al enfrentarse al *phishing* o a la ingeniería social.

Accenture y Ponemon también evalúan las prácticas de gobierno de ambos tipos de empresa, señalando que las que han dado el salto evolutivo están capacitadas para ofrecer informes periódicos sobre el estado de la seguridad, al tiempo que son más propensas a adoptar parámetros para la evaluación de las operaciones de seguridad, a realizar *benchmarking* de éstas frente a otros grupos de referencia y a llevar a cabo revisiones *post-mortem* de compromisos de seguridad y de incidentes en torno a la privacidad de los datos.

Finalmente, el estudio demuestra la confianza y la percepción que las empresas no estáticas en sus políticas de ciberseguridad tienen en la disminución de las disrupciones significativas (descendió un 49,4% en dos años, por un aumento en las organizaciones estáticas, en las que ascendió un 5,7%), del robo de datos (-46,4% frente a +12,5%) y de brechas en la infraestructura TI que alberga la información (-36,1% frente a 5,1%).

Mayor eficacia

Ahondando en esta idea de evolución empresarial, Accenture apunta tres enfoques claves para las organizaciones a la hora de plantearse la defensa frente a ciberataques. Expuestos en su documento **"Continuous Cyber Attacks: Engaging Business Leaders for the New Normal"**, con ellos pretende dar una respuesta a la situación actual, en la que las necesidades de cumplimiento regulatorio se anteponen a la gestión eficaz de riesgos y en las que las adquisiciones de productos y aplicaciones de seguridad drenan rápidamente los presupuestos destinados a la seguridad.

Las tres aproximaciones que Accenture propone son las siguientes:

– Participar activamente para hacer del negocio un mejor "cliente" de seguridad, mediante una mayor implicación del CISO en la alta dirección; una mejor articulación de los temas de seguridad en toda la estructura empresarial; y la desaparición de la ambigüedad en el momento de afrontar

cualquier amenaza, ya que el equipo de seguridad ha de saber quién es el "dueño" del sistema comprometido para potenciar la eficacia de la respuesta.

– **Fortalecer la colaboración entre el negocio y la seguridad**, a través de mantener la ciberseguridad en la "agenda" de la empresa (hay que tener en cuenta que tarde o temprano va a existir una brecha); de reconocer la complejidad del desafío que supone; de trabajar en equipo; y de evolucionar la cultura de la organización para atraer y retener el talento en lo que se refiere a seguridad de primer nivel.

– **Realizar continuos ejercicios de defensa**, como es el caso de tests que no se basen en la protección estática de la organización; de acciones de "caza" dentro de las defensas de la empresa, asumiendo que la seguridad se verá comprometida continuamente por intrusos; y de la mejora de la respuesta efectiva apoyándose en un equipo de élite capaz de evaluar las tácticas que llevan a cabo los atacantes.

Una visión de futuro

Más allá de acompañar a sus clientes hacia una evolución en materia de ciberseguridad poniendo como ejemplo el trabajo de otras empresas que ya han recorrido ese camino, Accenture también enfoca su capacidad analítica en prever lo que el mercado deparará a medio y largo plazo. En su informe "Security Implications of the Accenture Technology Vision" precisamente ofrece eso: su visión de lo que está por venir en torno a la seguridad.

Concretamente, Accenture afronta este año poniendo foco en cinco temas (todos ellos relacionados con la movilidad y la nueva realidad empresarial) con el objetivo de ayudar a las organizaciones a ampliar sus límites digitales.

• **Autonomía del borde**. ¿Qué impacto tiene en la seguridad la utilización de dispositivos IoT (en el límite de la organización) de cara a utilizarlos como parte de la toma de decisiones de negocio?

• **Integridad de los datos**. ¿Cómo hacer posible que las empresas se aseguren de que pueden confiar en los datos obtenidos de IoT para realizar analítica sobre ellos?

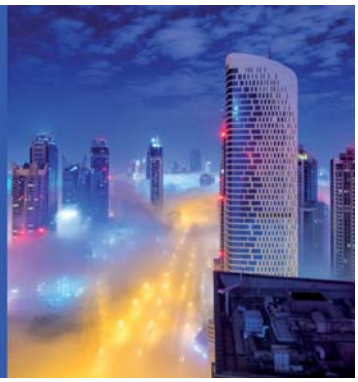
• **Seguridad Big Data**.¿Qué controles de seguridad son imprescindibles para proteger las iniciativas de *Big Data*, de manera que contribuyan al negocio sin aumentar su superficie de riesgo?

• **Plataformas de seguridad**. ¿Cómo pueden las empresas aprovechar sus plataformas para operar con seguridad en un ecosistema digital más amplio?

• **La confianza del cliente**. ¿Qué enfoques de seguridad y privacidad refuerzan la confianza del cliente en la era de la hiper-personalización? ●

Tendencias en ciberseguridad

- Mayor presión regulatoria.
- Apuesta por soluciones de seguridad integradas.
- Adopción de servicios de seguridad gestionada.
- Crecimiento de las capacidades de seguridad móviles y en la nube.
- Mayor enfoque en la detección y respuesta.
- Infraestructuras críticas e Internet de las Cosas.



"Empresas innovadoras" frente a "empresas estáticas"

	Empresas que dan el salto para mejorar su eficiencia en seguridad	Empresas estáticas
Estrategia	Establecen una estrategia de seguridad alineada con los objetivos empresariales y enfocada en la innovación para lograr una postura fuerte en seguridad. Consideran la innovación como un factor clave en el desarrollo de estrategias sostenibles que se adaptan al ritmo de evolución de las necesidades del negocio y, de este modo, ofrecen medidas de seguridad efectivas. La seguridad es una prioridad que cuenta con programas y presupuesto dedicado, un ecosistema fuerte (incluyendo la externalización de la seguridad) y una clara visión de seguir avanzando.	Operan la seguridad sin que repercuta de manera relevante en el funcionamiento diario de la empresa. Hay escasez de fondos para ello. Se basan en normativas y regulaciones, y no estrategia, como base para establecer sus requerimientos de seguridad. Son más propensas a centrarse en la prevención en lugar de en la detección proactiva o la contención de las amenazas una vez que estas se materializan.
Tecnología	Desarrollan capacidades de seguridad al tiempo que preservan la calidad de la experiencia del usuario y su productividad. Utilizan tecnología para permitir la detección de anomalías, priorizando amenazas, vulnerabilidades y ataques, así como desplegar controles para prevenir fugas de información y hacer la seguridad más adaptativa en el perímetro. Mejoran su capacidad para contrarrestar amenazas avanzadas. Están comprometidas con tecnologías nuevas y disruptivas, por ejemplo en torno a la nube y las comunicaciones.	Son menos proactivas a la hora de cambiar su enfoque de seguridad cuando se producen amenazas emergentes. Están convencidas de que los aspectos prioritarios se limitan a: controlar los dispositivos móviles inseguros (incluyendo BYOD), limitar el acceso a dispositivos potencialmente inseguros y disponer de funcionalidades potentes de *backup*.
Gobierno	Mejorar la eficiencia de la seguridad requiere un liderazgo fuerte y un claro alineamiento con el negocio. El CISO tiene la autoridad para definir y administrar la estrategia de seguridad, y ha establecido un canal de comunicación directo con el CEO y la Junta Directiva.	El CISO no tiene la autoridad para establecer una estrategia, ni una comunicación fluida con la Junta y el CEO. El gobierno y los controles son menos eficaces y la seguridad es considerada como un compromiso para la productividad de los empleados.

Tabla 1

BPO, Cloud e Infraestructura: la combinación perfecta para que tu negocio llegue a lo más alto.

Hemos combinado nuestra amplia experiencia en procesos de negocio con innovadores servicios de Infraestructura y Cloud. Es una capacidad única que nos permite desarrollar tus procesos y ofrecer servicios a medida que añadan un nuevo valor a tu empresa e impulsen su productividad. Nuestra red Global de Centros de Desarrollo y nuestra amplia experiencia en todos los sectores, nos permite ayudar a tu organización no solo a reducir gastos, sino también a generar ingresos y hacer que tu negocio llegue a lo más alto. Eso es alto rendimiento, hecho realidad.

Alto rendimiento. Hecho realidad.

Estrategia | Consultoría | Digital | Tecnología | Operaciones

accentureoperations