Competencias de Ciberseguridad de Insight

Insight

Introducción

La ciberseguridad es más crucial que nunca para todas las empresas, sea cual sea su tamaño, dado que la frecuencia y la sofisticación de las ciberamenazas van en aumento. Las brechas de ciberseguridad pueden tener consecuencias devastadoras, como pérdidas financieras, responsabilidades legales, daños a la marca y pérdida de confianza de los clientes.

Proteger a su empresa de las ciberamenazas no es sólo una cuestión de cumplimiento o de buenas prácticas; es esencial para salvaguardar sus operaciones y garantizar la continuidad del negocio.

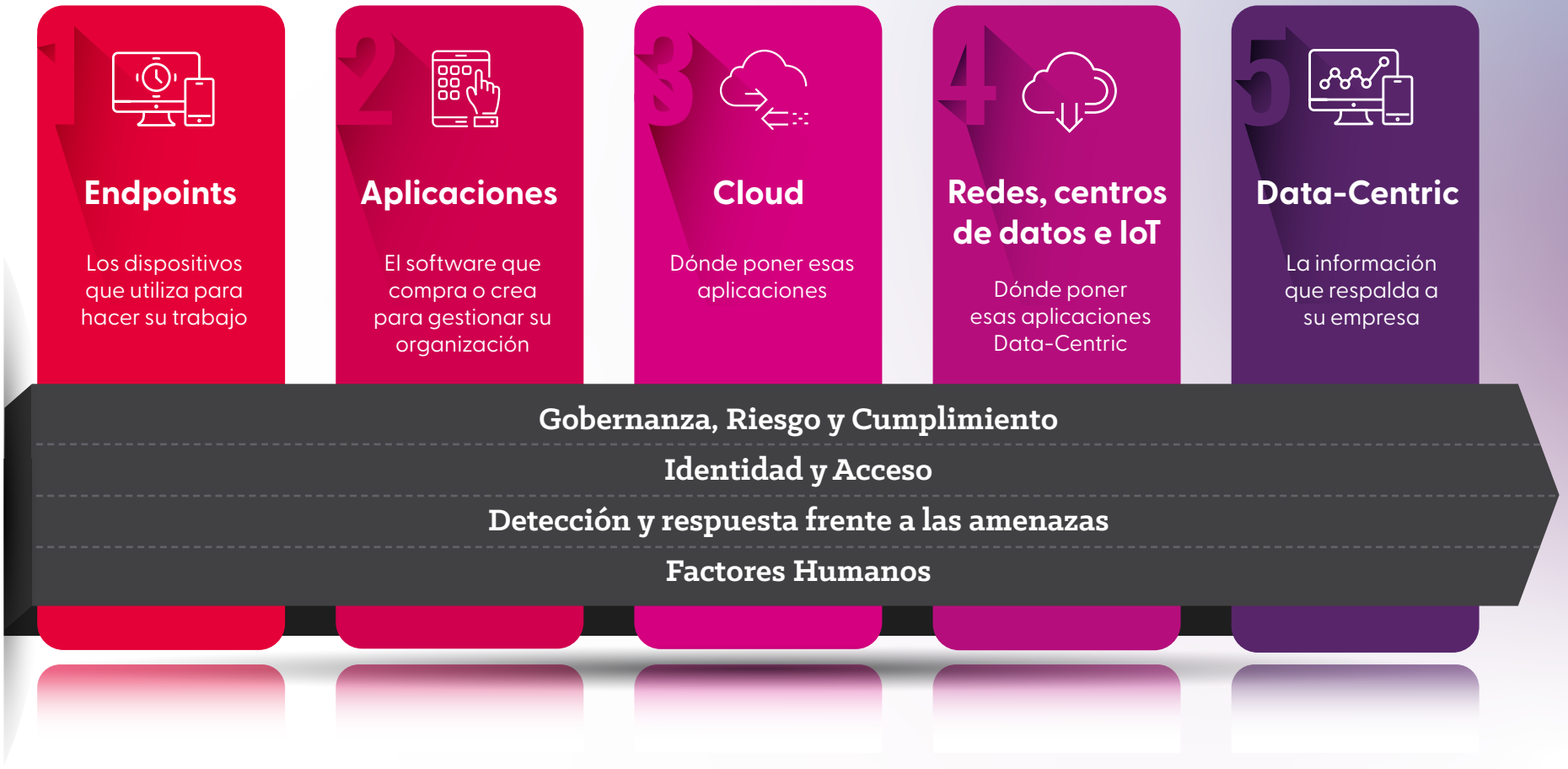
Invertir en medidas sólidas de ciberseguridad es invertir en la resiliencia y el éxito futuros de su empresa. Mediante la implementación de estrategias eficaces de ciberseguridad, se pueden mitigar los riesgos, detectar y responder a las amenazas a tiempo y construir una sólida defensa contra los ciberataques. La ciberseguridad no es sólo una necesidad; es un imperativo estratégico para las empresas que desean prosperar en un entorno seguro y resiliente.

En Insight somos conscientes de la necesidad de un enfoque integral de la seguridad.

El enfoque de Insight hacia la ciberseguridad

La ciberseguridad es complicada, lo que exige un enfoque integral por parte de los usuarios finales, los equipos de seguridad y las herramientas. Por eso, adoptamos un enfoque holístico de la ciberseguridad, tanto en el ámbito tecnológico como en el de la integración, a través de métodos repetibles y procesos probados que producen resultados satisfactorios. Nuestros expertos le guiarán de principio a fin para mejorar la eficiencia, la eficacia y la alineación estratégica.

Modelo de seguridad integral de Insight



El enfoque de Insight hacia la ciberseguridad

Contamos con amplias competencias técnicas en las cinco áreas de tecnología:

- Endpoints
- Aplicaciones
- Cloud
- Redes, centros de datos e IoT
- Data centric

pero, como integrador de soluciones líder, comprendemos que la excelencia técnica en estos ámbitos no es suficiente. La seguridad debe abordarse de forma holística, garantizando que todas las áreas de seguridad estén integradas y coordinadas. Lo hacemos mediante la aplicación de:

- Gobernanza, Riesgo y Cumplimiento
- Identidad y Acceso
- Detección y Respuesta frente a las Amenazas
- Factores Humanos

En las brechas en las que se entrecruzan los dominios tecnológicos es donde se puede obtener un valor añadido que ayude a mejorar su postura general de seguridad de forma rentable.

Esto, lo hacemos mediante la aplicación de:

- Mejorar la postura de ciberseguridad.
- Identificar y mitigar los riesgos
- Reducir la complejidad minimizando los solapamientos de tecnologías.
- Optimizar las operaciones de seguridad
- Garantizar que los controles de seguridad añaden valor y mejoran el rendimiento del gasto.

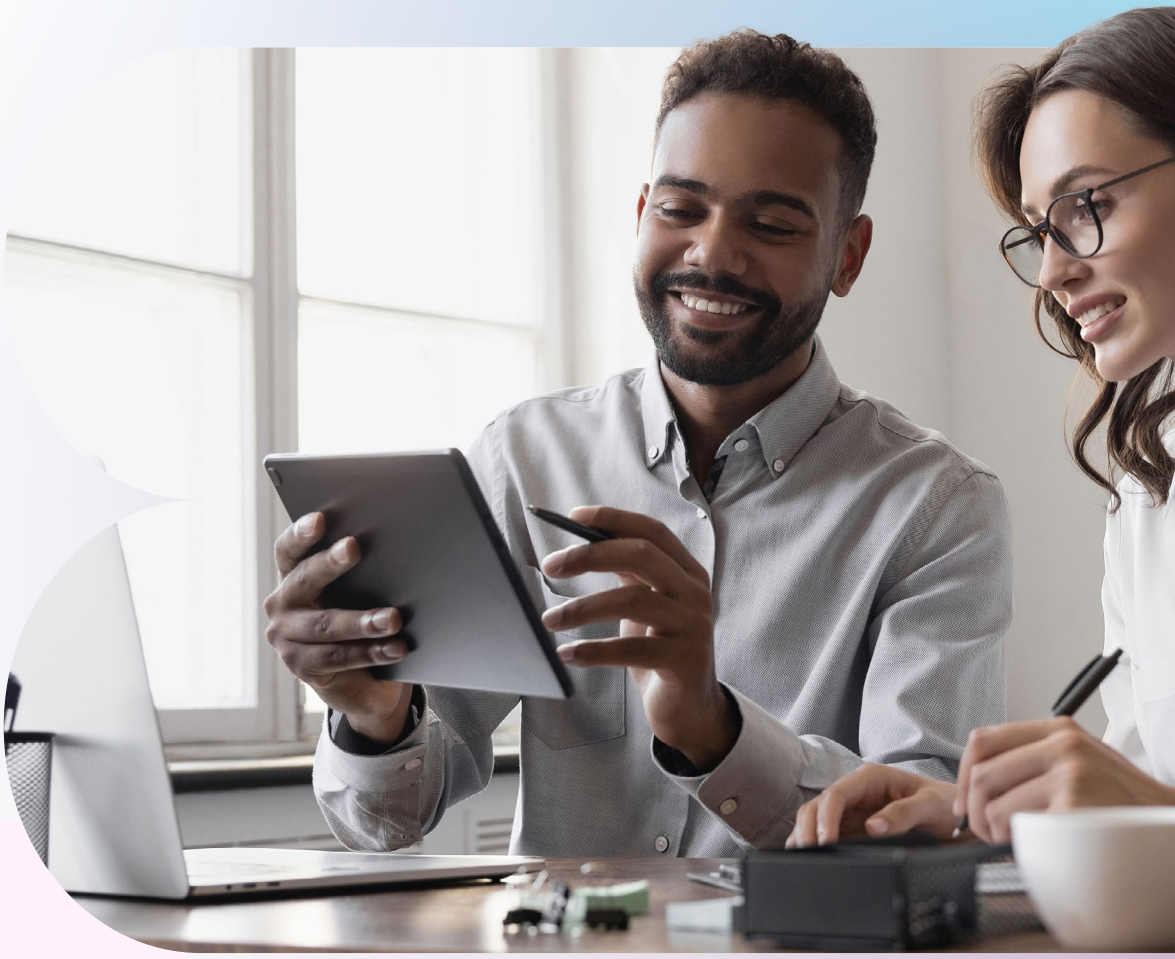
Los pilares de la tecnología

Endpoints

Atrás quedaron los días de un único dispositivo por usuario dentro de una empresa, es una realidad que sus empleados utilizan múltiples dispositivos. Los Endpoints desempeñan un papel fundamental en la ciberseguridad de las organizaciones, ya que sirven como puntos de entrada para las ciberamenazas y las vulnerabilidades. Los retos a la hora de proteger los endpoints han aumentado debido a la proliferación de dispositivos, los entornos de trabajo remotos y la creciente sofisticación de los ciberataques contra ellos.

Entre los retos más comunes se encuentran la visibilidad de los endpoints, la gestión de vulnerabilidades, la protección de datos y el control de aplicaciones.

Hay que gestionar estos dispositivos, supervisar y actualizar su seguridad e implantar y mantener defensas activas para bloquear el malware y los exploits. Nuestras soluciones de seguridad para endpoints se centran en el proceso de proteger terminales como portátiles, ordenadores de sobremesa, servidores y dispositivos móviles que se utilizan para acceder a las redes y los datos de la empresa.



Le ayudamos a:

- Obtener visibilidad de su entorno de endpoints, a nivel de dispositivos y aplicaciones.
- Detectar y responder a las ciberamenazas en tiempo real.
- Proteger los datos confidenciales de los dispositivos frente a accesos no autorizados.
- Prevenir las infecciones por malware y los ciberataques en los endpoints.
- Ganar visibilidad de las actividades de los endpoints para una supervisión eficaz.
- Asegurar dispositivos para entornos de trabajo remotos.

Aplicaciones

Con la constante evolución de las ciberamenazas, las organizaciones se enfrentan a importantes retos. Esto se ve agravado por el hecho de que la complejidad de las aplicaciones modernas es cada vez mayor, con numerosos componentes interconectados e integraciones de terceros, lo que da lugar a una mayor superficie de ataque. Los hackers y los ciberdelincuentes desarrollan continuamente nuevas técnicas para explotar las vulnerabilidades de las aplicaciones.

Todas las empresas utilizan aplicaciones que necesitan parches para mantenerse al tanto de las vulnerabilidades, tanto en los puestos de usuario como en la infraestructura de servidores. Asimismo, muchas organizaciones crearán sus propias aplicaciones, ya sea a través de código bajo/sin código o mediante desarrollo tradicional o DevOps. Integrar la seguridad y la privacidad desde el diseño en el ciclo de vida del desarrollo de software es fundamental para estas organizaciones.

Nuestro equipo de consultores de expertos en seguridad puede ayudarle a reducir los riesgos en la infraestructura de sus aplicaciones. Le ayudaremos a mantenerse al día con la gestión de vulnerabilidades y parches para sus aplicaciones, así como a proporcionar revisiones de código automatizadas y protección en tiempo de ejecución para cualquier aplicación web creada internamente.
Confíe en Insight para hacer frente a los retos de seguridad de sus aplicaciones, proporcionándole una protección sólida y tranquilidad.

Le ayudamos a:

- Gestionar su patrimonio de aplicaciones para mantenerse al tanto del ciclo de vulnerabilidades y parches.
- Integrar controles de seguridad en sus procesos de DevOps sin comprometer la velocidad de desarrollo.
- Invertir en la detección y corrección de amenazas, reduciendo el coste de la corrección.

Cloud

La computación cloud ofrece una escalabilidad y eficiencia inigualables, pero también presenta retos de seguridad significativos. Las empresas necesitan proteger sus datos confidenciales de accesos no autorizados, infracciones y vulnerabilidades, cumpliendo al mismo tiempo la normativa y salvaguardando la reputación de la empresa.

Es importante adoptar un enfoque proactivo y basado en los riesgos, colaborando con sus proveedores de nube para establecer un marco de seguridad sólido.

Los expertos en nube y seguridad de Insight cuentan con años de experiencia en la creación, la protección y el funcionamiento de entornos multicloud para organizaciones de todos los tamaños y complejidades. Le ayudaremos a crear un marco de seguridad integral con supervisión proactiva para que pueda centrarse en el crecimiento, la escalabilidad y las innovaciones.

Le ayudamos a:

- Obtener visibilidad de todo su entorno multicloud.
- Asegurar las cargas de trabajo dondequiera que se creen.
- Supervisar y mantener el cumplimiento normativo respecto a los marcos de seguridad.

Datacentre, red e IoT

En el actual mundo interconectado, el panorama digital se expande rápidamente, creando una compleja red tecnológica que ha abierto la puerta a un aumento de las ciberamenazas, las violaciones de datos y los accesos no autorizados.

Para construir las defensas de seguridad y la resistencia de las empresas de hoy en día se necesita un enfoque multicapa. Una combinación de cortafuegos, cifrado, controles de acceso y auditorías periódicas de seguridad es sólo el principio. Debe adelantarse continuamente a las amenazas con sistemas avanzados de detección de amenazas y análisis de expertos para ser proactivo en la identificación y mitigación de riesgos potenciales.

Adoptamos un enfoque consultivo para resolver sus retos de seguridad en centros de datos, redes e IoT. Con un profundo conocimiento de la empresa, la tecnología y la seguridad, creamos la solución adecuada para su negocio: desde la estrategia y la planificación con diseño, hasta la implantación y los servicios gestionados. Nuestros expertos en seguridad pueden ayudarle a navegar por la complejidad de la tecnología necesaria para crear y gestionar defensas de ciberseguridad eficaces, minimizando los solapamientos y ofreciendo una defensa de ciberseguridad rentable.

Le ayudamos a:

- Comprender arquitecturas híbridas complejas.
- Mejorar la continuidad operativa.
- Hacer funcionar los controles de seguridad tanto en sus redes locales como en la cloud.
- Mantener sus datos seguros de origen a destino.

Data-Centric

Aunque los profesionales de seguridad dedican mucho tiempo a proteger las aplicaciones y la infraestructura, en última instancia, casi todo lo que hacen se reduce a proteger los datos. Ya se trate de información sobre empleados, pedidos de clientes, cifras de producción o propiedad intelectual, son los datos que circulan por su empresa los que probablemente aportan más valor a sus clientes finales y a su negocio, y los que presentan más riesgos si se ponen en peligro.

Un buen punto de partida a la hora de pensar en su estrategia de seguridad holística son los datos, y un enfoque centrado en ellos debe empezar por implicar a las partes interesadas de su empresa, no por la tecnología.

Nuestro enfoque se centra en proteger los datos en sí, en lugar de simplemente proteger los sistemas o redes que los almacenan y transmiten. Le ayudamos a adelantarse a los acontecimientos y a proteger eficazmente el activo más valioso de su organización.

Le ayudamos a:

- Descubrir los datos sensibles y obsoletos de todo su patrimonio.
- Ayudar a clasificar los datos para garantizar que se aplica la cantidad correcta de control.
- Cumplir de la normativa sobre protección de datos.
- Auditar el uso de los datos

Dominios de integración

Gobernanza, Riesgo y Cumplimiento

La gobernanza, el riesgo y el cumplimiento son componentes esenciales de la ciberseguridad para las empresas, que abarcan las políticas, los procedimientos y los mecanismos para gestionar los riesgos de ciberseguridad y garantizar el cumplimiento de los requisitos reglamentarios, como GDPR y NIS2. Las organizaciones se enfrentan a dificultades a la hora de establecer estructuras de gobernanza eficaces, identificar y evaluar los riesgos de ciberseguridad y aplicar controles sólidos para mitigar las amenazas.

Las prácticas eficaces de GRC establecen funciones claras, agilizan los procesos y mitigan los riesgos cibernéticos. Un enfoque sólido aumentará la madurez de su ciberseguridad, reducirá las responsabilidades legales y financieras, mejorará la confianza de sus clientes y el cumplimiento de la normativa.

Insight le ayuda a garantizar que la seguridad satisface las necesidades de su empresa, en lugar de limitarlas. Utilizando evaluaciones de riesgos de seguridad para calcular el coste de ese riesgo y determinar dónde deben colocarse los controles para obtener los mejores resultados, garantizando al mismo tiempo que los controles seleccionados cumplen su función con eficacia.

Le ayudamos con:

- La evaluación de riesgos
- La definición de controles más eficaces
- El desarrollo de políticas y procesos
- Expertos integrados en todos los niveles de la organización, hasta el nivel de CISO.

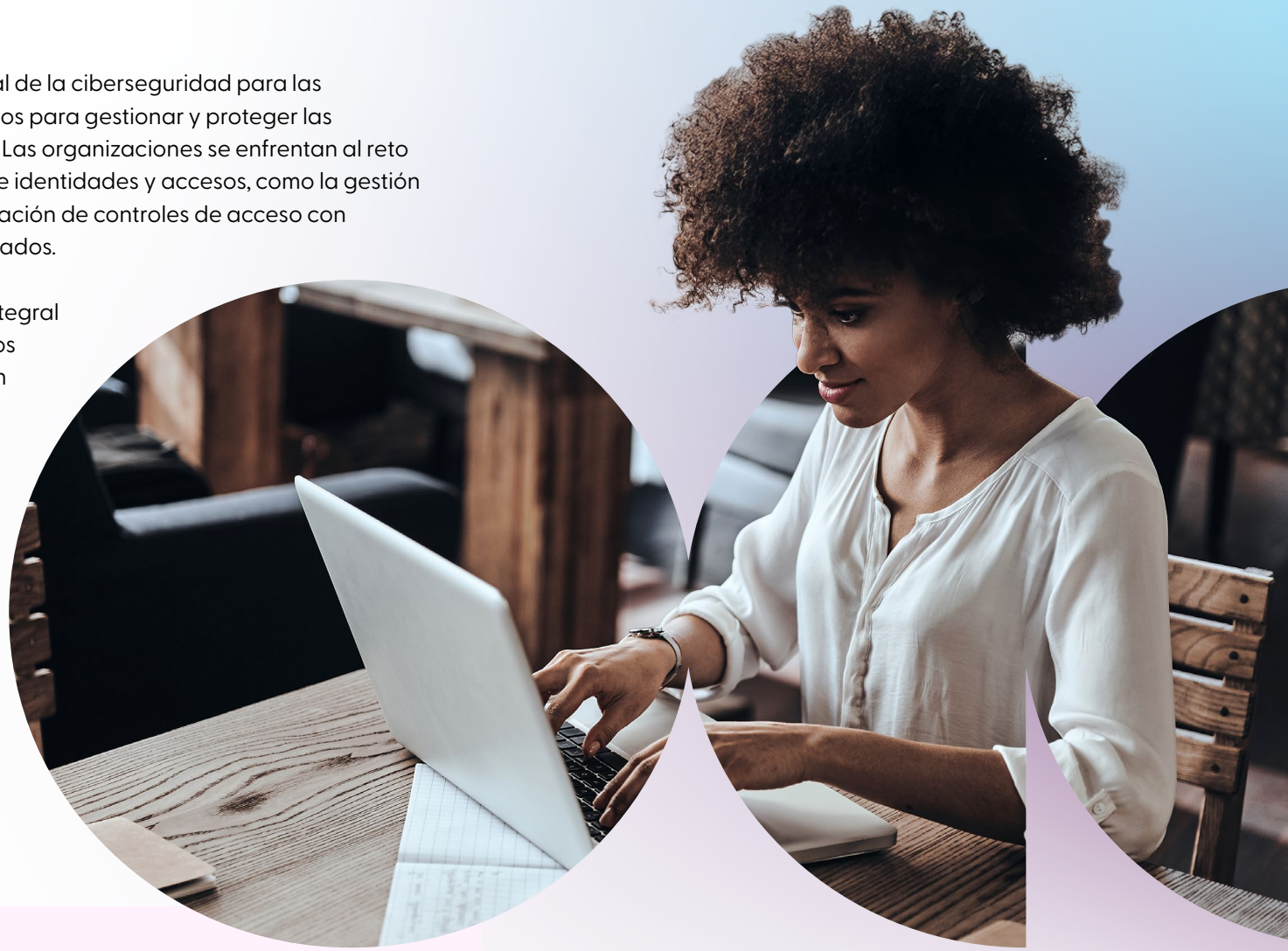
- **NIS / NIS2**
- **DORA**
- **Ley de IA de la EU**
- **ISO27001**
- **Ciberesenciales**
- **CIS18**
- **NIST CSF**
- **PCI-DSS**

Identidad y acceso

La gestión de identidades y accesos es un aspecto crucial de la ciberseguridad para las empresas, que abarca los procesos y tecnologías utilizados para gestionar y proteger las identidades digitales y controlar el acceso a los recursos. Las organizaciones se enfrentan al reto de garantizar prácticas seguras y eficientes de gestión de identidades y accesos, como la gestión de identidades de usuarios en múltiples sistemas, la aplicación de controles de acceso con privilegios mínimos y la prevención de accesos no autorizados.

Para ser eficaces, las empresas necesitan una solución integral de gestión de identidades y accesos desplegada en todos sus pilares tecnológicos, con el fin de ofrecer una solución cibernética sólida y completa.

El equipo de expertos en ciberseguridad de Insight le ayuda centrándose en identificar y mitigar las áreas de riesgo y, a continuación, le asiste en la creación de soluciones rentables que cumplan los requisitos de las políticas y procesos de su organización. El enfoque de Insight, adaptado a su empresa, le permitirá aumentar la seguridad, reducir los riesgos y mejorar la eficacia.t.



Lo logramos mediante:

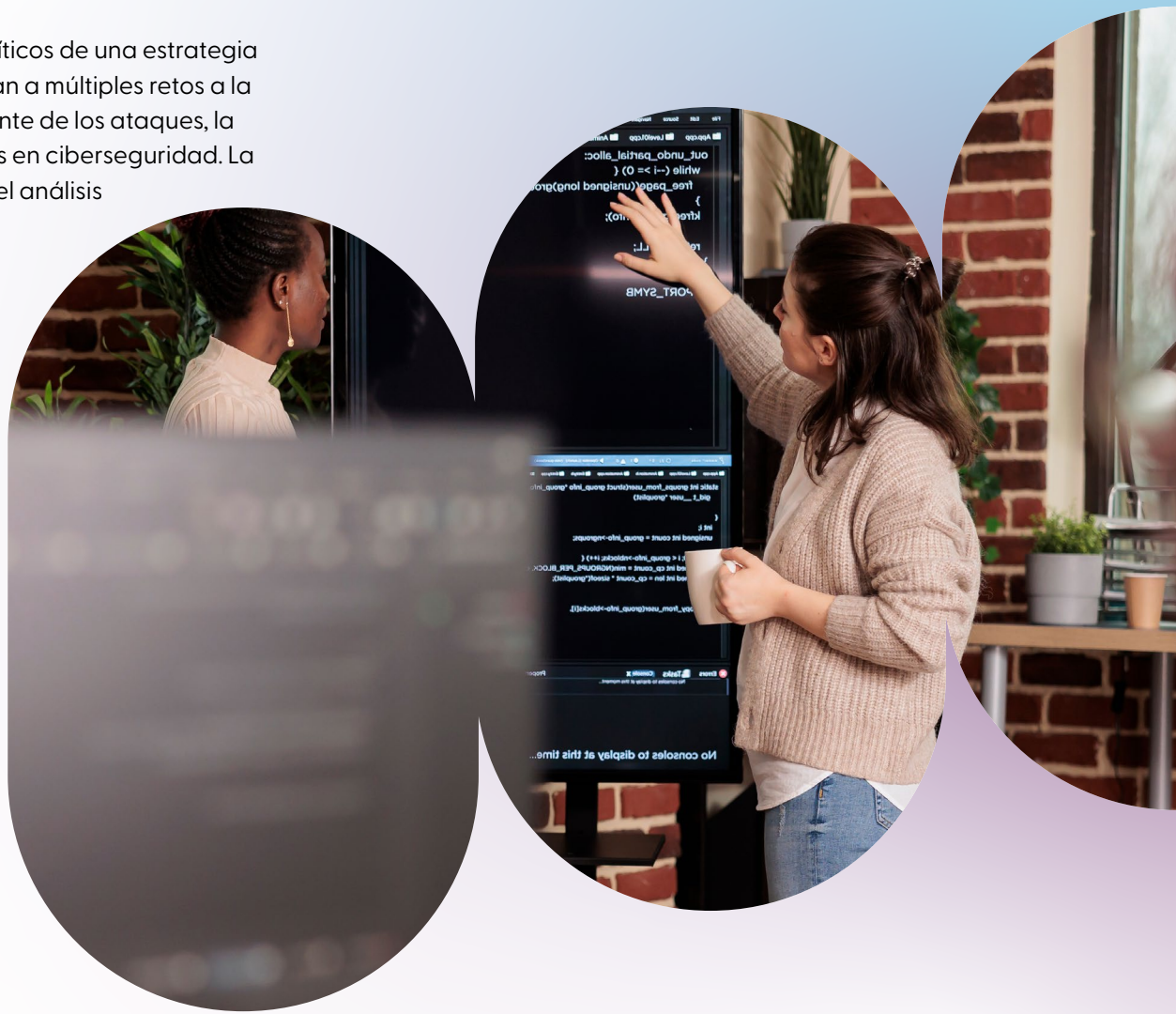
- El soporte en el camino hacia la confianza cero
- La adopción de un enfoque empresarial sobre el acceso a los datos y las aplicaciones
- La garantía de que sólo las personas adecuadas tengan acceso a sus aplicaciones y datos.

Detección y respuesta frente a las amenazas

La detección de amenazas y la respuesta a las mismas son componentes críticos de una estrategia de ciberseguridad sólida para las empresas. Las organizaciones se enfrentan a múltiples retos a la hora de identificar y mitigar las ciberamenazas, como la naturaleza cambiante de los ataques, la complejidad de los entornos de TI y la escasez de profesionales cualificados en ciberseguridad. La detección eficaz de las amenazas requiere una supervisión en tiempo real, el análisis de los eventos de seguridad y una respuesta rápida a los incidentes para minimizar el impacto de las brechas de seguridad.

Los expertos en seguridad de Insight pueden ayudarle a adoptar un enfoque multicapa para la detección de amenazas y soluciones de respuesta en todos los dominios tecnológicos de su empresa.

Creamos soluciones utilizando herramientas avanzadas, tecnologías y la experiencia de nuestros consultores de seguridad para identificar y mitigar los riesgos antes de que causen daños significativos a su empresa. Insight utiliza tecnologías como SIEM y XDR, reforzadas por analistas de seguridad, para reunir las enormes cantidades de datos generados por sus herramientas de seguridad y tomar decisiones inteligentes sobre amenazas y respuestas en todo su entorno.



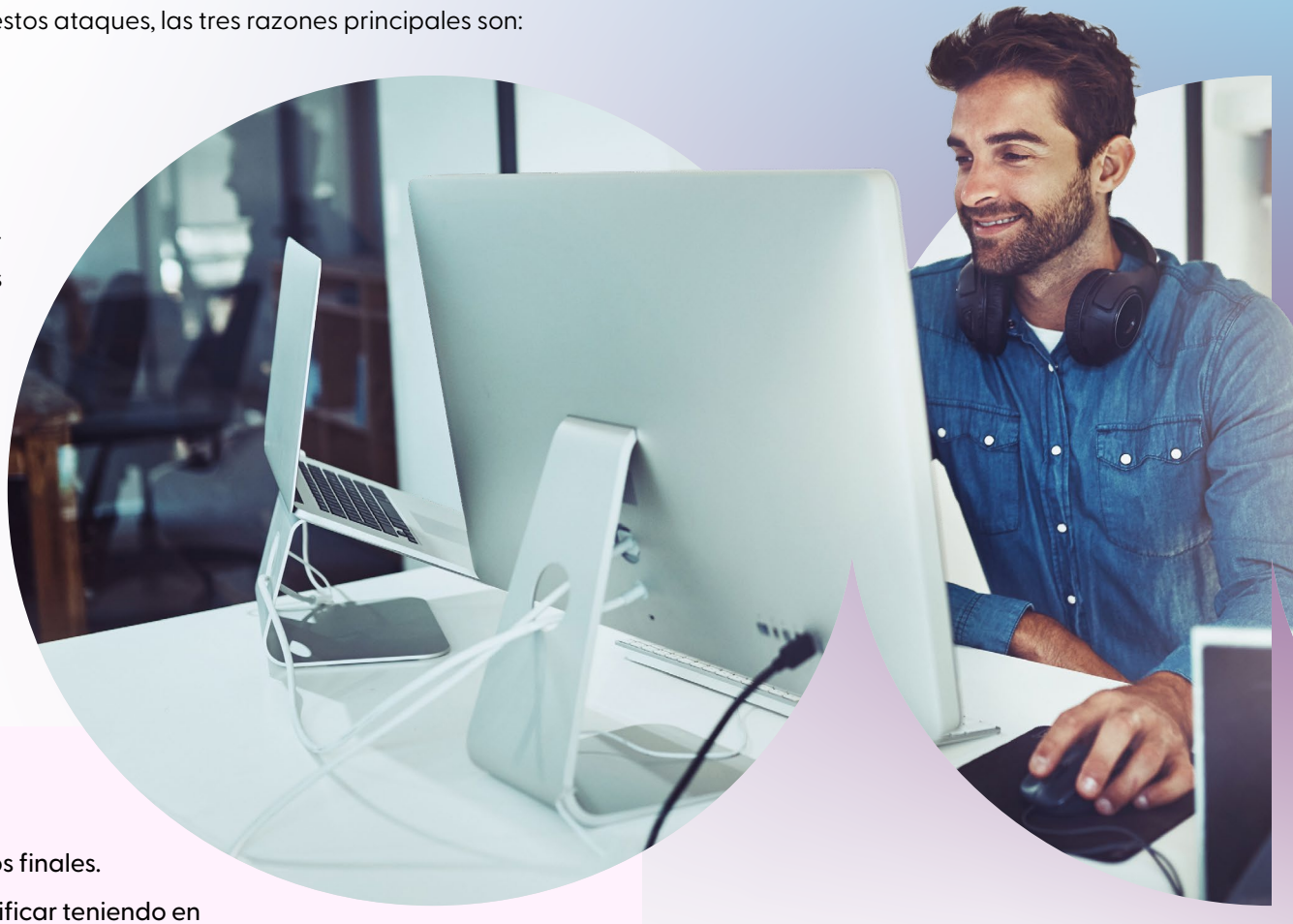
Le ayudamos a:

- Identificar las amenazas con antelación
- Reproducir los riesgos en toda la red
- Proporcionar información procesable sobre amenazas
- Automatizar la defensa contra amenazas

Factores Humanos

Aunque la infraestructura, las herramientas y los controles de seguridad se mejoran y se invierte continuamente en ellos, siguen produciéndose infracciones, y no son fáciles de identificar y resolver. Existen muchos controles de seguridad especializados para distintos tipos de amenazas, desde ataques a puntos finales hasta ataques a cadenas de suministro, pero cuando se examina cómo se producen estos ataques, las tres razones principales son:

- **Contraseñas**
- **Phishing**
- **Implementación de parches**



Los equipos de TI pueden utilizar la tecnología para ayudar a reducir las posibilidades de que se produzcan infracciones, pero los usuarios finales siempre tendrán un papel que desempeñar en el apoyo a la seguridad de una organización. Los equipos de TI a menudo se concentran en la tecnología, a veces en el proceso, y descuidan el factor humano, que puede determinar el fracaso o el éxito de un proyecto.

Capacite a sus empleados para convertirse en una impenetrable primera línea de defensa contra las ciberamenazas con Insight. Al adoptar un enfoque centrado en el ser humano, podemos ayudarle a hacer frente a las vulnerabilidades de forma directa, reforzando su postura de seguridad y minimizando los riesgos.

Le ayudaremos a:

- Mejorar la concienciación sobre ciberseguridad de los usuarios finales.
- Proporcionar formación a los desarrolladores sobre cómo codificar teniendo en cuenta la seguridad.
- Asegurar que sus administradores tengan las habilidades necesarias para detectar y responder a un ciberataque.
- Reducir los riesgos de ataques exitosos.
- Ahorrar costes evitando filtraciones de datos.

Seguridad gestionada

La avalancha de problemas de seguridad es incesante, y las empresas se enfrentan a un aumento cada vez mayor de las ciberamenazas, desde sofisticados intentos de pirateo hasta insidiosos ataques de ransomware. Las empresas deben cumplir complejos requisitos normativos, proteger datos confidenciales y anticiparse a los riesgos de ciberseguridad en constante evolución. Las soluciones de seguridad proporcionan numerosas alertas y alarmas, pero saber sobre cuáles actuar con urgencia es la clave para evitar daños mayores a su empresa.

La combinación de estos retos crea la necesidad de ofrecer soluciones de ciberseguridad completas y proactivas para proteger a las empresas de las diversas y sofisticadas amenazas a las que se enfrentan a diario. La preparación y la resistencia en materia de ciberseguridad son fundamentales para proteger la continuidad y el éxito de cualquier empresa moderna.

Ahí es donde Insight puede ayudarle: nuestro equipo de expertos en seguridad está disponible las 24 horas del día, los 7 días de la semana, para ayudarle a mejorar su ciberseguridad mediante la supervisión, detección y respuesta proactiva ante amenazas con acceso a tecnologías de vanguardia.

Nuestro Centro de Operaciones de Seguridad (SOC) ofrece dos ofertas de servicios gestionados que proporcionan capacidades avanzadas de detección, investigación y respuesta ante amenazas:

- **Detección y respuesta gestionadas para endpoints (MEDR)** Cubre portátiles, ordenadores de sobremesa y dispositivos móviles.
- **Detección y respuesta ampliadas gestionadas (MXDR)** Reúne registros y feeds de una amplia gama de fuentes, ofreciendo la capacidad de detección más sólida para su entorno.

Combinando tecnologías como la IA, el análisis y la inteligencia sobre amenazas, nuestro equipo de expertos analistas de seguridad puede detectar y responder a las amenazas a su entorno en tiempo real

Lo logramos mediante:

- La gestión proactiva de las actualizaciones
- La realización de un análisis de seguridad experto y con respuesta
- a incidentes
- El acceso a tecnologías de seguridad avanzadas
- El asesoramiento sobre la estrategia de seguridad y la hoja de ruta a seguir
- Modelos rentables y escalables

Cómo funcionamos

Le ayudaremos a diseñar estrategias, implantar y gestionar soluciones de TI preparadas para el futuro.

Evaluación

- Le ayudamos a obtener la acreditación con arreglo a marcos del sector como ISO27001 o NIS2.
- Revisar los controles de seguridad existentes e identificar los riesgos residuales
- Crear una hoja de ruta prioritaria para lograr el nivel de seguridad deseado

Planificación y diseño

- Asistencia para traducir sus retos empresariales en proyectos de seguridad soporte y orientación para seleccionar los proveedores, productos y servicios adecuados
- Talleres de previsión y diseño técnico

Construcción e implementación

- Convertir los planes en realidad: desde el diseño hasta los controles de seguridad totalmente construidos y documentados.
- Insight considera cada proyecto en el contexto de su hoja de ruta global transfiere a sus equipos internos la gestión o la transición a nuestros servicios gestionados.

Centro de operaciones de seguridad

- Servicios de asistencia para que sus controles de seguridad funcionen a pleno rendimiento
- Servicios gestionados en los que Insight se responsabiliza de sus controles de seguridad

Nuestros Partners Tecnológicos de Seguridad

La modernización de las TI es un trabajo de equipo. Unimos las capacidades de más de 6.000 partners y editores de software, hardware y nube con la amplia experiencia en el sector de nuestro equipo bajo un mismo techo para crear las mejores soluciones que aceleren su viaje de transformación.

Trabajamos directamente con empresas tecnológicas líderes para que pueda beneficiarse de:

- Un único punto de contacto para acceder a los últimos productos y soluciones tecnológicas.
- Un ecosistema de equipos de colaboración altamente cualificados para equipar y gestionar su entorno de TI.
- Precios competitivos y negociación de contratos simplificada.
- Soluciones independientes de los partners adaptadas a sus necesidades específicas.

Microsoft · cisco · aws · Google · paloalto NETWORKS

KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD. · FORTINET

¿Por qué asociarse con Insight?

La ciberseguridad es complicada, lo que exige un enfoque integral por parte de los usuarios finales, los equipos de seguridad y las herramientas. Por este motivo, hemos desarrollado métodos repetibles y procesos probados que ofrecen resultados satisfactorios. Nuestros expertos le guiarán de principio a fin para mejorar la eficiencia, la eficacia y la alineación estratégica.

Contamos con:

+20 años de conocimientos y experiencia en transformación de la seguridad

Profundas asociaciones con proveedores de primer nivel

Un enfoque agnóstico para encontrar las soluciones que mejor se ajusten a sus necesidades.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Gold Microsoft Partner
Microsoft
Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Próximos pasos

Póngase en contacto con Insight para mejorar su estrategia de ciberseguridad y sus operaciones diarias. Con el aumento de las amenazas a la ciberseguridad, proteger su empresa es crucial para la continuidad y el éxito. Nuestro enfoque integral mejora la postura de ciberseguridad, identifica y mitiga los riesgos, agiliza las operaciones, optimiza los controles de seguridad y maximiza las inversiones. Confíe en los métodos probados y la orientación experta de Insight para reforzar sus defensas de ciberseguridad e impulsar la resiliencia y el crecimiento empresarial.

- **es.insight.com**
- **0344 846 3333**