Ciberataques, IA y Estrategia

Informe de Ciberseguridad de 2025

excelia

Informe de Ciberseguridad 2025

El año 2025 ha marcado un punto de inflexión en el panorama global de la ciberseguridad. **La evolución acelerada de las amenazas, impulsada por la Inteligencia Artificial, la automatización y la creciente interconexión digital, ha transformado la naturaleza de los ciberataques, ampliando su alcance, sofisticación e impacto sobre organizaciones de todos los sectores.** Los incidentes ya no se limitan a compromisos técnicos aislados, sino que afectan de forma directa a la continuidad del negocio, la confianza de clientes y ciudadanos, el cumplimiento normativo y la estabilidad de infraestructuras críticas.

En este contexto, los ataques a la cadena de suministro, el ransomware orientado a la extorsión de datos, el robo masivo de credenciales y el fraude corporativo mediante deepfakes se han consolidado como vectores predominantes, poniendo de manifiesto que la superficie de ataque de las organizaciones se extiende más allá de sus propios sistemas hacia todo su ecosistema digital. Al mismo tiempo, **la entrada en vigor de nuevas regulaciones y marcos normativos** ha incrementado la visibilidad de los incidentes y elevado el nivel de exigencia en materia de gestión del riesgo y resiliencia operativa.

Este informe analiza los principales incidentes de ciberseguridad ocurridos en 2025, las tendencias más relevantes por región y sector, el impacto creciente de la Inteligencia Artificial tanto en ciberataques como en la defensa, y las claves estratégicas que marcarán las prioridades de ciberseguridad en 2026. Su objetivo es ofrecer una **visión clara y estructurada del escenario actual,** ayudando a las organizaciones a comprender los riesgos reales a los que se enfrentan y a tomar decisiones informadas para **proteger sus activos, garantizar la continuidad del negocio y fortalecer su posición** en un entorno digital cada vez más complejo y hostil.

Incidentes de ciberseguridad más importantes de 2025

El año 2025 estuvo marcado por una clara evolución en el perfil de las amenazas, con un foco creciente en ataques a la **cadena de suministro, proveedores tecnológicos y entornos de infraestructura crítica.** Los atacantes priorizaron vectores indirectos, explotando la confianza depositada en terceros y logrando así un impacto sistémico superior al de los ataques tradicionales directos. Esta tendencia confirmó que la superficie de ataque de las organizaciones ya no se limita a sus propios sistemas, sino que se extiende a todo su ecosistema digital.

©Excelia 2026. Todos los derechos reservados.

Informe de Ciberseguridad 2025

SECTOR PÚBLICO

España

En el ámbito del sector público español, uno de los incidentes más relevantes se produjo en enero de 2025, cuando una brecha de seguridad en un proveedor externo de servicios TI derivó en la **exposición de información sensible** vinculada a la Guardia Civil y las Fuerzas Armadas. Aunque los sistemas nucleares no fueron comprometidos directamente, el incidente evidenció debilidades en los controles de seguridad exigidos a terceros y en los mecanismos de supervisión y auditoría de proveedores críticos.

A nivel de administraciones locales, el Ayuntamiento de Badajoz sufrió en abril un ataque de ransomware atribuido al grupo LockBit, que provocó la paralización de numerosos servicios digitales municipales durante varios días. El ataque afectó a trámites administrativos, sistemas internos de gestión y comunicaciones, generando un impacto operativo significativo y obligando a activar planes de contingencia manuales. Este caso puso de manifiesto la especial **vulnerabilidad de las entidades locales,** que suelen contar con menos recursos especializados en ciberseguridad y mayores dependencias de proveedores externos.

En agosto de 2025, el Ayuntamiento de Elche fue víctima de un ciberataque grave que paralizó todos los sistemas informáticos municipales, obligando a suspender plazos administrativos y trasladar procedimientos a atención presencial mientras se contenía el incidente. Otros municipios, como Melilla, Níjar, La Rinconada o La Vila Joiosa, sufrieron ataques similares, con **sistemas cifrados por ransomware,** afectando servicios digitales y trámites ciudadanos.

Portugal

En Portugal, durante 2025 se registraron incidentes significativos de ciberseguridad que afectaron al sector público, destacando un ataque de ransomware a la Agência para a Modernização Administrativa (AMA). **Este incidente comprometió temporalmente varios servicios electrónicos críticos del Estado,** incluidos sistemas de autenticación digital como Autenticação.Gov y Gov.ID, interrumpiendo el acceso de ciudadanos y empleados públicos a servicios esenciales.

La respuesta al incidente estuvo coordinada por la AMA junto con el Centro Nacional de Cibersegurança (CNCS) y su equipo de respuesta ante emergencias informáticas (CERT.PT), quienes supervisaron la mitigación y recuperación de los sistemas afectados. Este caso evidenció la exposición del sector público portugués frente a ataques de ransomware y la importancia de reforzar la resiliencia digital de plataformas críticas.

Latinoamérica

En América Latina, el sector público fue uno de los principales objetivos de ciberataques durante 2025, con incidentes que afectaron a ministerios, gobiernos locales y servicios públicos esenciales. En Uruguay, un ataque al Ministerio de Desarrollo Social en el mes de abril provocó la **filtración de decenas de miles de documentos con datos personales de ciudadanos,** mientras que otros portales institucionales fueron comprometidos, evidenciando debilidades en la protección de sistemas gubernamentales.

En Brasil, varios ayuntamientos y administraciones locales sufrieron ataques de ransomware que paralizaron sistemas administrativos, servicios sociales y plataformas de atención ciudadana, obligando a suspender trámites y activar procedimientos manuales. El impacto fue especialmente significativo en el ámbito municipal, donde los recursos en ciberseguridad suelen ser más limitados.

Asimismo, el sector público sanitario también se vio afectado. En Perú, un hospital público fue víctima de un ataque de ransomware que comprometió sistemas clínicos y administrativos, poniendo de relieve el riesgo que estos incidentes suponen para la continuidad de servicios esenciales. En conjunto, estos casos reflejan un escenario de creciente exposición del sector público latinoamericano frente a amenazas cada vez más sofisticadas y persistentes.

Informe de Ciberseguridad 2025

SECTOR FINANCIERO Y SERVICIOS

El sector financiero y de grandes servicios también se vio especialmente afectado por incidentes relacionados con la gestión de datos y accesos a través de terceros. En junio de 2025, Telefónica notificó incidentes vinculados a la gestión y exposición de datos, lo que reavivó el debate sobre la protección de grandes volúmenes de información en entornos complejos y altamente interconectados.

Posteriormente, en noviembre, entidades financieras de primer nivel como ING y Banco Santander comunicaron accesos no autorizados originados en proveedores o servicios subcontratados. Aunque el impacto directo sobre clientes fue contenido, estos incidentes reforzaron la percepción de riesgo sistémico asociado a la externalización de servicios tecnológicos. El sector confirmó que **incluso organizaciones con elevados niveles de madurez en ciberseguridad pueden verse comprometidas si los controles de terceros no están alineados con sus propios estándares.**

En Latinoamérica, uno de los casos más significativos se registró en Brasil durante junio y julio de 2025, cuando el proveedor tecnológico C&M Software, autorizado por el Banco Central para conectar bancos y fintechs al sistema de pagos instantáneos PIX, fue comprometido por ciberdelincuentes. **Los atacantes obtuvieron credenciales legítimas y realizaron transacciones fraudulentas,** desviando cientos de millones de reales desde cuentas de reserva de varias instituciones hacia cuentas controladas por los criminales. Este incidente afectó a múltiples bancos y obligó al Banco Central a desconectar temporalmente el acceso de C&M al sistema, evidenciando la **vulnerabilidad de la infraestructura financiera frente a ataques a proveedores críticos.**

INDUSTRIA INTERNACIONAL Y TECNOLOGÍA OPERATIVA (OT)

En el ámbito industrial, uno de los casos más significativos fue el sufrido por Jaguar Land Rover, que se vio obligada a detener parte de su producción durante varias semanas tras un ataque dirigido contra sus sistemas de Tecnología Operativa (OT). A diferencia de los ataques puramente IT, este incidente tuvo **consecuencias directas sobre la continuidad del negocio, afectando a líneas de producción, logística y cadenas de suministro globales.**

Las pérdidas asociadas al lucro cesante, junto con los costes de recuperación y refuerzo de los sistemas industriales, ascendieron a cifras millonarias. Este incidente consolidó la preocupación del sector manufacturero por la convergencia IT/OT y la necesidad de reforzar la segmentación de redes, la monitorización de entornos industriales y los planes de respuesta ante incidentes específicos para OT.

FRAUDE CORPORATIVO MEDIANTE IA Y DEEPFAKES

Finalmente, 2025 supuso la consolidación del fraude corporativo basado en Inteligencia Artificial, especialmente mediante técnicas de deepfake en tiempo real. Durante el año se documentó un caso relevante en una multinacional, comparable en sofisticación al conocido caso Arup de años anteriores, en el que un empleado realizó una transferencia de fondos tras una videollamada aparentemente legítima con el CFO de la compañía.

La llamada había sido generada mediante IA, replicando con gran precisión la imagen, voz y gestos del directivo, lo que permitió superar los controles humanos tradicionales basados en reconocimiento visual y confianza jerárquica. **Este tipo de incidentes evidenció que los procedimientos clásicos de autorización ya no son suficientes y que el factor humano se ha convertido en uno de los principales objetivos de los atacantes,** obligando a las organizaciones a redefinir sus controles antifraude y procesos de verificación.

Informe de Ciberseguridad 2025

Estadísticas de ciberataques más extendidos en 2025

Los datos de 2025 reflejan una automatización masiva de los vectores de ataque, impulsada por tecnologías avanzadas y el uso de Inteligencia Artificial. Entre los incidentes más frecuentes, destacan los siguientes:

Phishing y Smishing

+1265%

Interanual

Estos ataques registraron un aumento interanual del 1265%, debido principalmente al uso de Modelos de Lenguaje (LLMs) para generar correos electrónicos y mensajes de texto de ingeniería social altamente personalizados, sin errores gramaticales y difíciles de detectar por los filtros convencionales.

Ransomware de extorsión de datos

35%

Incidentes graves

Representó aproximadamente el 35% de los incidentes graves. La tendencia predominante en 2025 fue abandonar el cifrado de sistemas a favor de la amenaza de publicación de datos sensibles, buscando extorsionar a las víctimas sin activar herramientas de detección anti-ransomware, lo que aumentó la efectividad y el riesgo reputacional para las organizaciones afectadas.

Ataques de identidad

+131%

Robo de credenciales

El robo de credenciales mediante infostealers creció un 131%, impulsado por el auge del mercado de "Access-as-a-Service" en la Dark Web, que facilita la venta de cuentas comprometidas y credenciales corporativas a actores maliciosos de todo el mundo.

Informe de Ciberseguridad 2025

> En conjunto, estas estadísticas muestran que 2025 ha sido un año de **sofisticación sin precedentes en los ataques cibernéticos,** caracterizado por la automatización, el uso de Inteligencia Artificial y la monetización de información sensible, lo que exige a las organizaciones reforzar sus mecanismos de prevención, detección y respuesta ante amenazas.

DATOS POR REGIÓN

Europa

En Europa, el panorama de ciberseguridad en 2025 estuvo marcado por la implementación de la directiva NIS2, que obligó a las organizaciones a notificar incidentes de manera más rigurosa. Esto se reflejó en un incremento del 43,2% en los incidentes reportados respecto a 2024, en gran parte debido a la obligatoriedad de notificación de la nueva normativa.

El foco de los ataques se concentró principalmente en las infraestructuras críticas, especialmente en los sectores de energía y telecomunicaciones, con ataques híbridos que combinan técnicas de intrusión digital y manipulación de sistemas operativos. Muchos de estos incidentes estuvieron vinculados a tensiones geopolíticas en el este del continente, mostrando cómo los conflictos internacionales influyen directamente en la ciberamenaza regional.

En España, aunque aún es pronto para tener las cifras oficiales de incidentes del Instituto Nacional de Ciberseguridad (INCIBE), su servicio de consultas de ciberseguridad ha superado las 114.863 consultas atendidas en 2025, cifra récord y que indica un aumento de los incidentes y preocupaciones relacionadas con seguridad digital en España.

+43,2%
Incidentes respecto a 2024

+114.863
Consultas a INCIBE

Informe de Ciberseguridad 2025

España ocupa el 7.º lugar en Europa entre los países más afectados por ciberataques en el periodo de análisis julio 2024–junio 2025, según el Microsoft Digital Defense Report.

Esto refleja la elevada exposición del país a incidentes de seguridad, especialmente en sectores críticos como energía, telecomunicaciones y servicios financieros, donde los ataques automatizados, el phishing y el ransomware siguen siendo los vectores predominantes.

Por su parte, Portugal se sitúa en la 12.ª posición europea, lo que también evidencia un aumento de la actividad maliciosa y la presión sobre infraestructuras críticas y empresas del país. Los incidentes reportados incluyen ataques sofisticados, campañas de ransomware y vulneraciones de credenciales, lo que confirma que ambos países ibéricos enfrentan un panorama de ciberamenazas complejo y en expansión.

Latinoamérica

Se ha consolidado en 2025 como la región con mayor crecimiento porcentual de ciberataques a nivel global, con un aumento del 108% en el número de ataques semanales respecto al año anterior. Este incremento refleja tanto la expansión de la digitalización en la región como la sofisticación creciente de los vectores de ataque, lo que ha colocado a América Latina en un escenario de riesgo muy elevado.

Los principales objetivos geográficos concentraron la mayor parte de las amenazas: Brasil, México y Colombia representaron el 86% de los ciberataques registrados en la región. La exposición de estos países se relaciona con la densidad de servicios financieros digitales, infraestructuras críticas y volumen de información sensible disponible en línea.

+108%

Ataques semanales respecto a 2024

86%

Ciberataques registrados en Brasil, México y Colombia

Informe de Ciberseguridad 2025

En cuanto a la tipología de los ataques, se observó una alta prevalencia de:

Troyanos bancarios móviles

Diseñados para robar credenciales de banca en línea y aplicaciones financieras, afectando principalmente a usuarios individuales y pequeñas empresas.

Malware

Distribuido mediante software pirata, que se propagó masivamente aprovechando la instalación de aplicaciones ilegales en entornos corporativos y domésticos.

Intentos de intrusión

A sistemas gubernamentales, con México registrando cifras récord, lo que evidenció un riesgo creciente para la continuidad de servicios públicos y la protección de datos ciudadanos.

Estos datos reflejan que Latinoamérica no solo experimentó un aumento en la cantidad de incidentes, sino también un cambio en la complejidad y el impacto potencial de los ataques, que afectaron tanto al sector financiero y empresarial como al sector público.

DATOS POR SECTOR

Durante el pasado año, el impacto y la frecuencia de los ciberataques variaron significativamente según el sector, reflejando tanto la exposición tecnológica como la criticidad de los activos afectados. Los datos globales muestran patrones claros de vulnerabilidad y riesgos económicos asociados a cada industria:

Educación e Investigación

4.484
Ataques semanales

Este sector lideró en volumen de incidentes, con un promedio de 4.484 ataques semanales por organización. La alta exposición se debe principalmente a los entornos abiertos y el uso masivo de dispositivos personales de estudiantes y personal académico, lo que facilita la propagación de malware y ataques de phishing dirigidos.

Gobierno y Militar

2.678
Incidentes semanales

Con 2.678 incidentes semanales por organización, este sector enfrenta riesgos derivados del ciberespionaje y el hacktivismo, donde actores estatales y grupos ideológicos buscan acceder a información sensible, interrumpir operaciones y minar la confianza en las instituciones.

Telecomunicaciones

2.664
Ataques semanales

Registraron un promedio de 2.664 ataques semanales, concentrados en infraestructura crítica que puede ser explotada para ataques de denegación de servicio distribuida (DDoS) o interrupción de servicios digitales esenciales. La dependencia de redes interconectadas hace que este sector sea un objetivo frecuente para ciberdelincuentes que buscan amplificación de impacto.

Informe de Ciberseguridad 2025

Salud

2.430
Incidentes semanales

Con 2.430 incidentes semanales, este sector se destacó por el alto impacto económico de los ataques. Cada registro médico robado o comprometido tiene un coste promedio superior al de otros sectores, lo que convierte a hospitales y laboratorios en objetivos prioritarios de ransomware y robo de datos.

Manufactura e Industria

1.585
Ataques semanales

Este sector registró 1.585 ataques semanales. Menor volumen, pero con un impacto operativo muy alto, ya que los ataques pueden provocar latencia crítica, interrupciones de producción y pérdidas millonarias en la cadena de suministro. Los sistemas de Tecnología Operativa (OT) resultan especialmente vulnerables a ataques dirigidos.

En conjunto, estos datos muestran que el volumen de ataques no siempre coincide con el impacto económico: mientras que educación e investigación enfrentan la mayor cantidad de incidentes, los sectores de salud e industrial registran los mayores costes asociados.

La guerra invisible de la IA: sofisticación ofensiva y defensiva proactiva

La Inteligencia Artificial está transformando el panorama de la ciberseguridad, generando una auténtica "carrera armamentística" entre atacantes y defensores. Mientras los ciberdelincuentes están aplicando la IA para automatizar y sofisticar sus ataques, las organizaciones están implementando algoritmos inteligentes para mejorar la detección de amenazas y la resiliencia operativa. Este proceso está cambiando la forma en que se crean, detectan y mitigan los ciberataques, aumentando tanto la velocidad como la complejidad de los incidentes y las defensas.

IA OFENSIVA

Los atacantes están utilizando la IA para desarrollar ataques más efectivos y difíciles de detectar. Entre los principales vectores de uso destacan:

Desarrollo de malware

Herramientas como WormGPT están generando código malicioso polimórfico que se adapta a diferentes entornos, evadiendo antivirus y sistemas tradicionales de detección.

Vishing automatizado

Sistemas de voz generativa están manteniendo conversaciones elefónicas con víctimas, con el objetivo de obtener códigos de autenticación bancaria (OTP) y credenciales, aumentando la efectividad de los ataques de ingeniería social.

Deepfakes y suplantación de identidad

Tecnologías de síntesis de voz e imagen están permitiendo crear ídeos y audios falsos de directivos y empleados, utilizados en fraudes financieros, ataques de Business Email Compromise (BEC) y engaños dirigidos a departamentos financieros y de recursos humanos. Estos ataques están elevando significativamente el nivel de credibilidad de las estafas y el riesgo económico asociado.

Informe de Ciberseguridad 2025

IA DEFENSIVA

Al mismo tiempo, las organizaciones están aplicando IA para optimizar la protección y anticipar ataques, gracias a la utilización de, entre otras, técnicas como estas:

Triaje automático de alertas

Herramientas como WormGPT están generando código malicioso polimórfico que se adapta a diferentes entornos, evadiendo antivirus y sistemas tradicionales de detección.

Análisis predictivo

Sistemas basados en User and Entity Behavior Analytics (UEBA) están detectando intrusiones mediante anomalías de comportamiento de usuarios, como patrones de acceso inusuales en tiempo o ubicación, permitiendo anticipar ataques antes de que se materialicen.

Tendencias en ciberseguridad en 2026

Para 2026, los analistas de mercado están proyectando cambios drásticos en las prioridades de ciberseguridad, impulsados por la evolución tecnológica, la sofisticación creciente de los ataques y la complejidad normativa global.

Las organizaciones están adaptando sus estrategias para enfrentar amenazas más inteligentes y persistentes, mientras buscan optimizar recursos y proteger activos críticos en un entorno digital cada vez más interconectado.

Al mismo tiempo, la transformación tecnológica está redefiniendo los conceptos tradicionales de perímetro de seguridad, identidad y control de accesos, obligando a empresas de todos los sectores a replantear la forma en que gestionan riesgos, vulnerabilidades y cumplimiento regulatorio.

©Excelia 2026. Todos los derechos reservados.

Entre las principales tendencias identificadas para 2026 se destacan:

CRIPTOGRAFÍA POST-CUÁNTICA (PQC)

Las organizaciones están iniciando la migración urgente de protocolos de cifrado tradicionales hacia soluciones resistentes a la computación cuántica, anticipando la amenaza de ataques tipo "Harvest Now, Decrypt Later", donde datos sensibles capturados hoy podrían ser descifrados en el futuro por ordenadores cuánticos.

GESTIÓN DE EXPOSICIÓN A AMENAZAS (CTEM)

Se está produciendo un cambio de enfoque en la gestión de vulnerabilidades: en lugar de aplicar parches de forma masiva e indiscriminada, las empresas están priorizando únicamente las vulnerabilidades realmente explotables en su contexto, optimizando recursos y reduciendo la superficie de riesgo.

IDENTIDAD UNIFICADA Y NUEVO PERÍMETRO DE SEGURIDAD

Con la desaparición progresiva del perímetro de red tradicional (VPN, firewalls), la identidad continua y biométrica se está consolidando como el principal control de acceso. La gestión de identidad y la confianza digital se están convirtiendo en el nuevo perímetro de seguridad, protegiendo tanto la información como los accesos frente a amenazas críticas como el robo de credenciales y la suplantación de identidad.

PLATAFORMIZACIÓN DE LA SEGURIDAD

Las empresas están reduciendo la fragmentación de herramientas, migrando de un ecosistema de múltiples soluciones diferentes a plataformas consolidadas de un solo proveedor. Esto facilita la gestión mediante IA y mejora la eficiencia operativa, reduciendo la complejidad de integración y supervisión.

Informe de Ciberseguridad 2025

EVOLUCIÓN DEL MODELO ZERO TRUST

El enfoque Zero Trust está evolucionando hacia un modelo proactivo y contextual, donde cada acceso se verifica de forma continua, considerando el comportamiento del usuario, la ubicación y el nivel de riesgo. Esto permite fortalecer la seguridad de manera dinámica y en tiempo real, anticipando posibles incidentes antes de que se materialicen.

CUMPLIMIENTO NORMATIVO COMO EJE ESTRATÉGICO

Regulaciones como NIS2, DORA, CRA, AI Act o CSRD se están integrando de forma nativa en procesos y sistemas, permitiendo a las empresas operar con mayor confianza, minimizar riesgos y reforzar su reputación frente a clientes, reguladores y stakeholders.

GESTIÓN DE RIESGOS EN LA CADENA DE PROVEEDORES

La monitorización de terceros y la implementación de mecanismos de ciberseguridad integrados se están convirtiendo en un requisito crítico para garantizar la continuidad y resiliencia del negocio. Dado que los riesgos externos y los incidentes en proveedores siguen creciendo en complejidad e impacto, las empresas están adoptando enfoques más estratégicos para proteger toda la cadena de suministro digital.

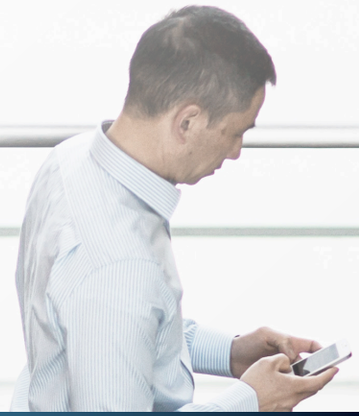
Seguridad que impulsa el negocio:

La visión de Excelia,

apostar por la ciberseguridad a día de hoy no es un gasto: **es una inversión estratégica.**

©Excelia 2026. Todos los derechos reservados.

Las empresas, sin importar su tamaño, se están enfrentando a un entorno donde los ciberataques no solo buscan acceder a datos, sino que comprometen la confianza del cliente, la reputación de marca y la resiliencia del negocio. La transformación digital, la migración masiva a la nube, la adopción de entornos multicloud e híbridos y la irrupción de la Inteligencia Artificial están ampliando la superficie de ataque y multiplicando los riesgos.



> La ciberseguridad ya no es únicamente un área de TI: se ha convertido en un pilar estratégico para toda la organización, involucrando a dirección, operaciones, recursos humanos y finanzas.

Cada decisión de negocio, cada dato compartido y cada interacción digital puede representar un punto de riesgo, por lo que **proteger la información y los sistemas se ha vuelto responsabilidad de todos,** y un factor clave para la continuidad, la confianza y la reputación de la empresa.

Informe de Ciberseguridad 2025

Los impactos de un incidente de seguridad se extienden a todos los niveles de la organización:

DIRECCIÓN Y GOBIERNO

Cumplimiento normativo (NIS2, DORA, GDPR), gestión de riesgos y estrategia de seguridad.

OPERACIONES

Continuidad de sistemas y procesos críticos, prevención de paradas en el servicio y pérdidas de productividad.

REPUTACIÓN Y MARKETING

Pérdida de confianza de clientes, ocios e inversores.

FINANZAS

Impacto directo de fraudes, ransomware y costes de recuperación.

PERSONAS Y CULTURA

Empleados como primera línea de defensa frente al phishing y la ingeniería social.

LEGAL Y COMPLIANCE

Sanciones por incumplimiento regulatorio.

La ciberseguridad debe entenderse como un valor de negocio, que protege activos, asegura el cumplimiento regulatorio y garantiza que la organización pueda operar y crecer en un entorno cada vez más hostil y regulado.

Informe de Ciberseguridad 2025

En Excelia entendemos que la seguridad de la información es clave para la continuidad y el éxito de cualquier empresa. Cada dato, conexión y dispositivo representa un activo estratégico que debe protegerse frente a amenazas cibernéticas en constante evolución. Nuestra propuesta de ciberseguridad va más allá de la tecnología: combinamos soluciones avanzadas con un enfoque integral que protege datos, redes, dispositivos, usuarios y aplicaciones, garantizando la continuidad del negocio y la confianza de tus clientes.

Con Excelia, la ciberseguridad se convierte en un aliado estratégico que permite a las empresas operar con seguridad, reducir riesgos y cumplir con los estándares más exigentes de protección de la información, transformando la inversión en ciberseguridad en un motor de resiliencia, confianza y crecimiento sostenido.

©Excelia 2026. Todos los derechos reservados.

Fuentes

Principales ciberataques de 2025

Detectados datos de personales supuestamente de la Guardia Civil y del Ministerio de Defensa en la dark web. INCIBE. **Ver**

El Ayuntamiento de Badajoz restablece la normalidad tras el ataque informático sufrido. Ayuntamiento de Badajoz. **Ver**

El Ayuntamiento registra un ataque informático que deja inoperativo el sistema informático municipal. Ayuntamiento de Elche. **Ver**

CNCS acompanha incidente de ransomware notificado pela AMA. Security Magazine. **Ver**

Nuevo ciberataque al Mides: filtraron más de 37.000 documentos con información personal de los ciudadanos. El País. **Ver**

Prefeitura de Porto Nacional é alvo de ataque hacker e sistemas saem do ar. Prefeitura Porto Nacional. **Ver**

Publicación de Prefeitura de Rio Preto. Facebook. **Ver**

Hospital José Agurto Tello de Chosica. Ransomware.Live. **Ver**

Telefónica investiga un supuesto 'hackeo' en Movistar que afectaría a 22 millones de registros de clientes. RTVE. **Ver**

ING España reconoce una filtración de datos de sus clientes. ADSLzone. **Ver**

Comunicado. Santander. **Ver**

Brazil's central bank vows tougher rules after surge in financial system cyberat-tacks. Reuters. **Ver**

Ciberataque paraliza las operaciones de Jaguar Land Rover. INCIBE. **Ver**

Fraude BEC en multinacional. INCIBE. **Ver**

Estadísticas globales y tendencias de ataque

Cyber Attack Trends. Check Point Research. **Ver**

State of Cybercrime. SentinelOne. **Ver**

Informe de Ciberseguridad 2025

Datos económicos y coste de brechas

Cost of a Data Breach Report. IBM Security. **Ver**

Allianz Risk Barometer. Allianz. **Ver**

Análisis regional

Threat Landscape. ENISA. **Ver**

Éxito en la campaña de publicidad del servicio 017. INCIBE. **Ver**

Microsoft Digital Defense Report 2025. Microsoft. **Ver**

FortiGuard Labs. Fortinet. **Ver**

Predicciones tecnológicas y estrategia 2026

Top Strategic Technology Trends. Gartner. **Ver**

Google Cloud Cybersecurity Forecast. Google. **Ver**

Normativa y sector público

CCN-CERT (Centro Criptológico Nacional - España). **Ver**

INCIBE (Instituto Nacional de Ciberseguridad). **Ver**

Soluciones de Excelia

Cybersecurity Solutions. Excelia. **Ver**

Excelia es una multinacional española de consultoría, tecnología y servicios profesionales con más de 25 años de experiencia en el mercado, con oficinas propias en 9 países y que opera en más de 50 a nivel global. Nuestro objetivo es ayudar a nuestros clientes a cumplir con sus retos empresariales, dando un paso más hacia un proceso de digitalización continua, a través de soluciones y servicios globales impulsados por la tecnología.

De esta forma, aseguramos un crecimiento sostenible a través de la innovación y apostando por nuevas tecnologías de vanguardia. Contamos con una amplia red de más de 300 profesionales repartidos por todo el mundo. Un equipo humano especializado y global, pero con conocimiento local, completamente comprometido con las necesidades de nuestros clientes.

Más información en www.excelia.com

info@excelia.com · 917 080 550
Paseo del Club Deportivo 1
Parque empresarial La Finca
Edificio 11, Planta 1
Pozuelo de Alarcón. Madrid

excelia