Ciberataques, IA e Estratégia

Relatório de Cibersegurança de 2025

excelia

Relatório de Cibersegurança de 2025

O ano de 2025 marcou um ponto de viragem no panorama global de cibersegurança. **A evolução acelerada das ameaças, impulsionada pela Inteligência Artificial, pela automação e pela crescente interligação digital, transformou a natureza dos ciberataques, ampliando o seu alcance, sofisticação e impacto nas organizações de todos os setores.** Os incidentes deixaram de se limitar a falhas técnicas isoladas, passando a afetar diretamente a continuidade do negócio, a confiança de clientes e cidadãos, o cumprimento regulatório e a estabilidade das infraestruturas críticas.

Neste contexto, os ataques à cadeia de abastecimentos, o ransomware orientado à extorsão de dados, o roubo massivo de credenciais e a fraude corporativa através de deepfakes consolidaram-se como vetores predominantes, evidenciando que a superfície de ataque das organizações já não se restringe aos seus próprios sistemas, estendendo-se a todo o ecossistema digital em que operam. Ao mesmo tempo, **a entrada em vigor de novos enquadramentos regulatórios e normativos** aumentou a visibilidade dos incidentes e elevou o nível de exigência em matéria de gestão de risco e de resiliência operacional.

Este relatório analisa os principais incidentes de cibersegurança registados em 2025, as tendências mais relevantes por região e setor, o impacto crescente da Inteligência Artificial tanto nos ciberataques como na defesa, bem como os fatores estratégicos que irão definir as prioridades de cibersegurança em 2026. O seu objetivo é oferecer uma **visão clara e estruturada do contexto atual,** ajudando as organizações a compreender os riscos reais a que estão expostas e a tomar decisões informadas para **proteger os seus ativos, garantir a continuidade do negócio e fortalecer a sua posição** num ambiente digital cada vez mais complexo e adverso.

©Excelia 2026. Todos os direitos reservados.

Principais incidentes de cibersegurança de 2025

O ano de 2025 foi marcado por uma clara evolução no perfil das ameaças, com um foco crescente em ataques à **cadeia de abastecimentos, a fornecedores de tecnologia e a ambientes de infraestrutura crítica.** Os atacantes passaram a priorizar vetores indiretos, explorando a confiança depositada em terceiros e alcançando, desta forma, um impacto sistêmico superior ao dos ataques diretos tradicionais. Essa tendência veio confirmar que a superfície de ataque das organizações já não se limita aos seus próprios sistemas, estendendo-se a todo o seu ecossistema digital.

©Excelia 2026. Todos os direitos reservados.

Relatório de Cibersegurança de 2025

SETOR PÚBLICO

Espanha

No âmbito do setor público espanhol, um dos incidentes mais relevantes ocorreu em janeiro de 2025, quando uma falha de segurança num fornecedor externo de serviços de TI resultou na **exposição de informação sensível** associada à Guardia Civil e às Forças Armadas. Embora os sistemas nucleares não tenham sido diretamente comprometidos, o incidente evidenciou fragilidades nos controlos de segurança exigidos a terceiros, bem como nos mecanismos de supervisão e auditoria de fornecedores críticos.

Ao nível da administração local, a Câmara Municipal de Badajoz foi alvo em abril de um ataque de ransomware atribuído ao grupo LockBit, que levou à paralisação de vários serviços digitais municipais durante vários dias. O ataque afetou procedimentos administrativos, sistemas internos de gestão e comunicações, gerando um impacto operacional significativo e obrigando à ativação de planos de contingência manuais. Este caso veio reforçar a especial **vulnerabilidade das entidades locais,** que geralmente dispõem de menos recursos especializados em cibersegurança e uma maior dependência de fornecedores externos.

Em agosto de 2025, a Câmara Municipal de Elche foi vítima de um ciberataque grave que paralisou todos os sistemas informáticos municipais, levando à suspensão de prazos administrativos e à transferência de procedimentos para atendimento presencial enquanto o incidente era controlado. Outros municípios, como Melilla, Níjar, La Rinconada e La Vila Joiosa, sofreram ataques semelhantes, com s**istemas encriptados por ransomware,** afetando serviços digitais e procedimentos essenciais para os cidadãos.

Portugal

Em Portugal, ao longo de 2025, registaram-se incidentes relevantes de cibersegurança que afetaram o setor público, destacando-se um ataque de ransomware à Agência para a Modernização Administrativa (AMA). **Este incidente comprometeu temporariamente vários serviços eletrónicos críticos do Estado,** incluindo sistemas de autenticação digital como Autenticação.Gov e Gov. ID, interrompendo o acesso de cidadãos e funcionários públicos a serviços essenciais.

A resposta ao incidente foi coordenada pela AMA em articulação com o Centro Nacional de Cibersegurança (CNCS) e sua equipa de resposta a emergências informáticas (CERT.PT), que supervisionaram as ações de mitigação e recuperação dos sistemas afetados. Este caso evidenciou a exposição do setor público português a ataques de ransomware e reforçou a importância de investir na resiliência digital das plataformas críticas.

América Latina

Na América Latina, o setor público foi um dos principais alvos de ciberataques em 2025, com incidentes que afetaram ministérios, governos locais e serviços públicos essenciais. No Uruguai, um ataque ao Ministério do Desenvolvimento Social ocorrido em abril resultou na **exposição de dezenas de milhares de documentos com dados pessoais de cidadãos,** enquanto outros portais institucionais foram comprometidos, evidenciando fragilidades na proteção dos sistemas governamentais.

No Brasil, várias câmaras municipais e administrações locais foram alvo de ataques de ransomware que paralisaram sistemas administrativos, serviços sociais e plataformas de atendimento ao cidadão, obrigando à suspensão de procedimentos e à ativação de processos manuais. O impacto foi particularmente significativo no âmbito municipal, onde os recursos em cibersegurança tendem a ser mais limitados.

Além disso, o setor público de saúde também foi afetado. No Peru, um hospital público foi vítima de um ataque de ransomware que comprometeu sistemas clínicos e administrativos, evidenciando o risco que esses incidentes representam para a continuidade de serviços essenciais. Em conjunto, estes casos refletem um cenário de crescente exposição do setor público latino-americano frente a ameaças cada vez mais sofisticadas e persistentes.

Relatório de Cibersegurança de 2025

SETOR FINANCEIRO E DE SERVIÇOS

O setor financeiro e de grandes serviços também foi fortemente afetado por incidentes relacionados à gestão de dados e acessos através de terceiros. Em junho de 2025, a Telefónica notificou incidentes associados à gestão e exposição de dados, reacendendo o debate sobre a proteção de grandes volumes de informação em ambientes complexos e altamente interligados.

Posteriormente, em novembro, instituições financeiras de primeira linha como ING e Banco Santander comunicaram acessos não autorizados com origem em fornecedores ou serviços subcontratados. Embora o impacto direto sobre os clientes tenha sido mitigado, estes incidentes reforçaram a perceção de risco sistêmico associada à externalização de serviços tecnológicos. O setor confirmou que **mesmo organizações com elevados níveis de maturidade em cibersegurança podem ser comprometidas se os controlos aplicados a terceiros não estejam alinhados com os seus próprios padrões.**

Na América Latina, um dos casos mais relevantes ocorreu no Brasil entre junho e julho de 2025, quando o fornecedor tecnológico C&M Software, autorizado pelo Banco Central a ligar bancos e fintechs ao sistema de pagamentos instantâneos PIX, foi comprometido por cibercriminosos. **Os atacantes obtiveram credenciais legítimas e realizaram transações fraudulentas,** desviando centenas de milhões de reais de contas de reserva de várias instituições para contas controladas pelos criminosos. Este incidente afetou múltiplos bancos e levou o Banco Central a desligar temporariamente o acesso da C&M ao sistema, evidenciando a **vulnerabilidade da infraestrutura financeira a ataques dirigidos a fornecedores críticos.**

INDÚSTRIA INTERNACIONAL E TECNOLOGIA OPERACIONAL (OT)

No contexto industrial, um dos casos mais relevantes foi o da Jaguar Land Rover, que se viu obrigada a interromper parte da sua produção durante várias semanas na sequência de um ataque dirigido aos seus sistemas de Tecnologia Operacional (OT). Ao contrário dos ataques exclusivamente de TI, este incidente teve **impactos diretos na continuidade do negócio, afetando linhas de produção, logística e cadeias de abastecimento globais.**

As perdas associadas ao lucro cessante, a par dos custos de recuperação e de reforço dos sistemas industriais, ascenderam a valores milionários. Este incidente veio reforçar a preocupação do setor industrial com a convergência IT/OT e a necessidade de reforçar a segmentação de redes, a monitorização de ambientes industriais e planos de resposta a incidentes específicos para OT.

FRAUDE CORPORATIVA ATRAVÉS DE IA E DEEPFAKES

Por fim, 2025 marcou a consolidação da fraude corporativa baseada em Inteligência Artificial, em particular através do uso de técnicas de deepfake em tempo real. Ao longo do ano, foi documentado um caso relevante numa multinacional, comparável em termos de sofisticação ao conhecido caso Arup de anos anteriores, no qual um colaborador realizou uma transferência de fundos após uma videoconferência aparentemente legítima com o CFO da organização.

A chamada foi gerada com recurso a IA, replicando com elevado grau de precisão a imagem, a voz e os gestos do executivo, o que permitiu ultrapassar os controlos humanos tradicionais baseados no reconhecimento visual e na confiança hierárquica. **Este tipo de incidentes evidenciou que os procedimentos clássicos de autorização já não são suficientes e que o fator humano se tornou um dos principais alvos dos atacantes,** obrigando as organizações a redefinir os seus controlos antifraude e processos de verificação.

Relatório de Cibersegurança de 2025

Estatísticas dos ciberataques mais frequentes em 2025

Os dados de 2025 refletem uma automação massiva dos vetores de ataque, impulsionada por tecnologias avançadas e pelo uso de Inteligência Artificial. Entre os incidentes mais frequentes, destacam-se os seguintes:

Phishing e Smishing

+1265%

Homólogo

Estes ataques registraram um aumento homólogo de 1265%, impulsionado sobretudo pela utilização de Modelos de Linguagem (LLMs) para gerar e-mails e mensagens de texto de engenharia social altamente personalizados, sem erros gramaticais e difíceis de detetar pelos mecanismos tradicionais de filtragem.

Ransomware de extorsão de dado

35%

Incidentes graves

Representou aproximadamente 35% dos incidentes graves. A tendência predominante em 2025 foi o abandono da encriptação dos sistemas em favor da ameaça de divulgação de dados sensíveis, com o objetivo de extorquir as vítimas sem acionar ferramentas de deteção anti-ransomware, o que aumentou significativamente a eficácia dos ataques e o risco reputacional para as organizações afetadas.

Ataques de identidade

+131%

Roubo de credenciais

O roubo de credenciais através de infostealers cresceu 131%, impulsionado pela expansão do mercado de "Access-as-a-Service" na Dark Web, que facilita a venda de contas comprometidas e credenciais corporativas a agentes maliciosos em todo o mundo.

Relatório de Cibersegurança de 2025

> Em conjunto, estas estatísticas evidenciam que 2025 foi um ano de **sofisticação sem precedentes nos ciberataques,** caracterizado pela automação, pelo uso de Inteligência Artificial e pela monetização de informações sensíveis, o que exige que as organizações reforcem os seus mecanismos de prevenção, deteção e resposta a ameaças.

DADOS POR REGIÃO

Europa

Na Europa, o panorama de cibersegurança em 2025 foi marcado pela implementação da diretiva NIS2, que obrigou as organizações a notificar incidentes de forma mais rigorosa. Esta medida refletiu-se num aumento de 43,2% nos incidentes reportados face a 2024, em grande parte devido à obrigatoriedade de notificação introduzida pela nova regulamentação.

O foco dos ataques concentrou-se principalmente em infraestruturas críticas, especialmente nos setores de energia e telecomunicações, com ataques híbridos que combinam técnicas de intrusão digital e manipulação de sistemas operacionais. Muitos desses incidentes estiveram associados a tensões geopolíticas no leste do continente, evidenciando o impacto direto dos conflitos internacionais no panorama regional de ciberameaças.

Em Espanha, embora ainda não estejam disponíveis os dados oficiais do incidentes do Instituto Nacional de Cibersegurança (INCIBE), o seu serviço de consultas de cibersegurança respondeu a mais de 114.863 solicitações em 2025, um valor recorde que demonstra um aumento dos incidentes e das preocupações relacionadas com a segurança digital no país.

+43,2%
Incidentes face a 2024

+114.863
Consultas a INCIBE

Relatório de Cibersegurança de 2025

Espanha ocupa o 7.º lugar na Europa entre os países mais afetados por ciberataques no período compreendido entre julho de 2024 e junho de 2025, de acordo com o Microsoft Digital Defense Report.

Este posicionamento reflete a elevada exposição do país a incidentes de segurança, em particular em setores críticos como energia, telecomunicações e serviços financeiros, onde ataques automatizados, phishing e ransomware continuam a ser os vetores predominantes.

Por sua vez, Portugal situa-se na 12.ª posição europeia, o que também evidencia um aumento da atividade maliciosa e da pressão sobre infraestruturas críticas e empresas do país. Os incidentes reportados incluem ataques sofisticados, campanhas de ransomware e violações de credenciais, confirmando que ambos os países ibéricos enfrentam um panorama de ciberameaças complexo e em expansão.

América Latina

A América Latina consolidou-se em 2025 como a região com maior crescimento percentual de ciberataques a nível global, com um aumento de 108% no número de ataques semanais face ao ano anterior. Este crescimento reflete tanto a expansão da digitalização na região como a crescente sofisticação dos vetores de ataque, colocando a América Latina num cenário de risco muito elevado.

Os principais alvos geográficos concentraram a maior parte das ameaças: Brasil, México e Colômbia representaram 86% dos ciberataques registrados na região. A exposição destes países está associada à densidade de serviços financeiros digitais, infraestruturas críticas e ao volume de informação sensível disponível online.

+108%

Ataque semanais face ao 2024

86%

Ciberataques registrados na Brasil, México e Colômbia

Relatório de Cibersegurança de 2025

Quanto à tipologia dos ataques, observou-se uma elevada prevalência de:

Trojans bancários móveis

Concebidos para roubar credenciais de bancos online e aplicações financeiras, afetando principalmente utilizadores individuais e pequenas empresas.

Malware

Distribuído através de software pirata, propagando-se massivamente devido a instalação de aplicações ilegais em ambientes corporativos e domésticos.

Tentativas de intrusão

Em sistemas governamentais, com o México a registar números recorde, evidenciando um risco crescente para a continuidade dos serviços públicos e a proteção dos dados dos cidadãos.

Estes dados indicam que a América Latina não apenas registou um aumento na quantidade de incidentes, mas também uma mudança na complexidade e no impacto potencial dos ataques, afetando simultaneamente o setor financeiro, empresarial e público.

Relatório de Cibersegurança de 2025

DADOS POR SETOR

Durante o ano passado, o impacto e a frequência dos ciberataques variaram significativamente consoante o setor, refletindo tanto a exposição tecnológica como a criticidade dos ativos afetados. Os dados globais mostram padrões claros de vulnerabilidade e riscos económicos associados a cada indústria:

Educação e Pesquisa

4.484
Ataques semanais

Este setor registou o maior volume de incidentes, com uma média de 4.484 ataques semanais por organização. A elevada exposição deve-se principalmente aos ambientes abertos e ao uso massivo de dispositivos pessoais por estudantes e pessoal académico, facilitando a propagação de malware e ataques de phishing direcionados.

Governo e Militar

2.678
Incidentes semanais

Com uma média de 2.678 incidentes semanais por organização, este setor enfrenta riscos associados à ciberespionagem e hacktivismo, em que atores estatais e grupos ideológicos procuram aceder a informação sensível, interromper operações e minar a confiança nas instituições.

Telecomunicações

2.664
Ataques semanais

Registaram uma média de 2.664 ataques semanais, concentrados em infraestruturas críticas que podem ser exploradas para ataques de negação de serviço distribuída (DDoS) ou interrupção de serviços digitais essenciais. A dependência de redes interconectadas torna este setor um alvo frequente para cibercriminosos que procuram amplificar o impacto dos ataques.

Saúde

2.430
Incidentes semanais

Com 2.430 incidentes semanais, este setor destacou-se pelo elevado impacto económico dos ataques. Cada registo médico roubado ou comprometido tem um custo médio superior ao de outros setores, tornando hospitais e laboratórios alvos prioritários de ransomware e roubo de dados.

Manufatura e Indústria

1.585
Ataques semanais

Este setor registrou 1.585 ataques semanais. Apesar do menor volume, apresenta um impacto operacional muito elevado, já que os ataques podem causar latência crítica, interrupções na produção e perdas milionárias na cadeia de fornecimento. Os sistemas de Tecnologia Operacional (OT) são especialmente vulneráveis a ataques direcionados.

Em conjunto, estes dados evidenciam que o volume de ataques nem sempre coincide com o impacto económico: enquanto educação e pesquisa enfrentam o maior número de incidentes, os setores de saúde e da indústria registaram os maiores custos associados.

A guerra invisível da IA: sofisticação ofensiva e defesa proativa

A Inteligência Artificial está a transformar o panorama da cibersegurança, gerando uma verdadeira "corrida armamentista" entre atacantes e defensores. Enquanto os cibercriminosos utilizam IA para automatizar e sofisticar os seus ataques, as organizações implementam algoritmos inteligentes para melhorar a deteção de ameaças e a resiliência operacional. Esse processo está a mudar a forma como os ciberataques são concebidos, detectados e mitigados, aumentando tanto a velocidade como a complexidade dos incidentes e das defesas.

IA OFENSIVA

Os atacantes estão a recorrer à IA para desenvolver ataques mais eficazes e difíceis de detetar. Entre os principais vetores de utilização destacam-se:

Desenvolvimento de malware

Ferramentas como o WormGPT estão a ser utilizadas para gerar código malicioso polimórfico que se adapta a diferentes ambientes, contornando antivírus e sistemas tradicionais de deteção.

Vishing automatizado

Sistemas de voz generativa permitem manter conversas telefónicas realistas com vítimas, com o objetivo de obter códigos de autenticação bancária (OTP) e credenciais, aumentando a eficácia dos ataques de engenharia social.

Deepfakes e usurpação de identidade

Tecnologias de síntese de voz e imagem permitem criar vídeos e áudios falsos de dirigentes e colaboradores, utilizados em fraudes financeiras, ataques de Business Email Compromise (BEC) e esquemas dirigidos a departamentos financeiros e de recursos humanos. Estes ataques aumentam substancialmente o nível de credibilidade das burlas e o risco económico associado.

Relatório de Cibersegurança de 2025

IA DEFENSIVA

Em paralelo, as organizações estão a aplicar IA para reforçar a proteção e antecipar ataques, recorrendo, entre outras, às seguintes abordagens:

Triagem automática de alertas

Os Centros de Operações de Segurança (SOC) estão a encerrar automaticamente 90% dos alertas de baixo risco, libertando os analistas para se concentrarem em incidentes de maior impacto.

Análise preditiva

Sistemas baseados em User and Entity Behavior Analytics (UEBA) permitem detetar intrusões através de anomalias no comportamento de utilizadores, como padrões de acesso invulgares em termos de horário ou localização, permitindo antecipar ataques antes que se materializem.

Tendências de Cibersegurança 2026

Para 2026, os analistas de mercado antecipam mudanças profundas nas prioridades de cibersegurança, impulsionadas pela evolução tecnológica, pela crescente sofisticação dos ataques e pela complexidade do enquadramento regulatório global.

As organizações estão a adaptar as suas estratégias para enfrentar ameaças mais inteligentes e persistentes, enquanto procuram otimizar recursos e proteger ativos críticos num ambiente digital cada vez mais interligado.

Em paralelo, a transformação tecnológica está a redefinir os conceitos tradicionais de perímetro de segurança, identidade e controlo de acessos, obrigando empresas de todos os setores a repensar a forma como gerem riscos, vulnerabilidades e conformidade regulatória.

©Excelia 2026. Todos os direitos reservados.

Relatório de Cibersegurança de 2025

Entre as principais tendências identificadas para 2026, destacam-se:

CRIPTOGRAFIA PÓS-QUÂNTICA (PQC)

As organizações estão a iniciar uma migração urgente de protocolos de criptografia tradicionais para soluções resistentes à computação quântica, antecipando a ameaça de ataques do tipo 'Harvest Now, Decrypt Later' (Recolher Agora, Decifrar Depois), onde dados sensíveis capturados hoje poderão ser decifrados no futuro através de computadores quânticos.

GESTÃO DE EXPOSIÇÃO A AMEAÇAS (CTEM)

Está a verificar-se uma mudança de paradigma na gestão de vulnerabilidades: em vez de aplicar correções (patches) de forma massiva e indiscriminada, as empresas estão a priorizar apenas as vulnerabilidades realmente exploráveis no seu contexto, otimizando recursos e reduzindo a superfície de risco.

IDENTIDADE UNIFICADA E NOVO PERÍMETRO DE SEGURANÇA

Com o desaparecimento progressivo do perímetro de rede tradicional (VPN, firewalls), a identidade contínua e biométrica está a afirmar-se como o principal controlo de acesso. A gestão de identidade e a confiança digital passam a constituir o novo perímetro de segurança, protegendo informação e acessos face a ameaças críticas, como o roubo de credenciais e a usurpação de identidade.

PLATAFORMIZAÇÃO DA SEGURANÇA

As empresas estão a reduzir a fragmentação de ferramentas, migrando de um ecossistema de 50 soluções diferentes para plataformas consolidadas de um único fornecedor. Esta abordagem facilita a gestão suportada por IA e melhora a eficiência operacional, reduzindo a complexidade de integração e supervisão.

EVOLUÇÃO DO MODELO ZERO TRUST

O modelo Zero Trust está a evoluir para uma abordagem proativa e contextual, onde cada acesso é verificado de forma contínua, considerando o comportamento do utilizador, a localização e o nível de risco. Esta evolução permite reforçar a segurança de forma dinâmica e em tempo real, antecipando potênciais incidentes antes que se materializem.

CONFORMIDADE REGULAMENTAR COMO EIXO ESTRATÉGICO

Regulamentações como NIS2, DORA, CRA, AI Act ou CSRD estão a ser integradas de forma nativa nos processos e sistemas, permitindo às empresas operar com maior confiança, minimizar riscos e reforçar a reputação junto de clientes, reguladores e stakeholders.

GESTÃO DE RISCOS NA CADEIA DE FORNECEDORES

A monitorização de terceiros e a implementação de mecanismos de cibersegurança integrados estão a tornar-se requisitos críticos para garantir a continuidade e a resiliência do negócio. Dado que os riscos externos e os incidentes em fornecedores continuam a crescer em complexidade e impacto, as organizações estão a adotar abordagens mais estratégicas para proteger toda a cadeia de fornecimento digital.

Segurança que impulsiona o negócio:

a visão da Excelia,

investir na cibersegurança hoje em dia não é um custo: **é um investimento estratégico.**

Investir na cibersegurança hoje em dia não é um custo: é um investimento estratégico. As organizações, independentemente da sua dimensão, enfrentam um contexto onde os ciberataques já não se limitam ao acesso indevido a dados, mas colocam em causa a confiança dos clientes, a reputação da marca e a resiliência do negócio. A transformação digital, a migração massiva para a cloud, a adoção de ambientes multicloud e híbridos e a crescente utilização da Inteligência Artificial estão a expandir significativamente a superfície de ataque e a multiplicar os riscos.

> A cibersegurança já não é apenas uma área de TI: tornou-se um pilar estratégico para toda a organização, envolvendo a direção, operações, recursos humanos e áreas financeiras

Cada decisão de negócio, cada dado partilhado e cada interação digital pode representar um ponto de risco, pelo que proteger a informação e os sistemas tornou-se responsabilidade de todos, e um fator crítico para a continuidade, a confiança e a reputação da empresa.

Relatório de Cibersegurança de 2025

Os impactos de um incidente de segurança estendem-se a todos os níveis da organização:

DIREÇÃO E GOVERNANÇA

Conformidade regulamentar (NIS2, DORA, GDPR), gestão de riscos e estratégia de segurança.

OPERAÇÕES

Continuidade de sistemas e processos críticos, prevenção de interrupções no serviço e perdas de produtividade.

REPUTAÇÃO E MARKETING

Perda de confiança de clientes, parceiros e investidores.

FINANÇAS

Impacto direto de fraudes, ransomware e custos de recuperação.

PESSOAS E CULTURA

Colaboradores como primeira linha de defesa contra o phishing e a engenharia social.

JURÍDICO E CONFORMIDADE (COMPLIANCE)

sanções por incumprimento regulamentar.

A cibersegurança deve ser encarada como um verdadeiro valor de negócio, que protege ativos, assegura a conformidade regulamentar e garante que a organização possa operar e crescer num ambiente cada vez mais complexo e regulado.

Relatório de Cibersegurança de 2025

Na Excelia, acreditamos que a segurança da informação é fundamental para a continuidade e o sucesso de qualquer organização. Cada dado, cada ligação e cada dispositivo representa um ativo estratégico que deve ser protegido face a ameaças cibernéticas em constante evolução. A nossa proposta de cibersegurança vai além da tecnologia: combinamos soluções avançadas com uma abordagem integrada que protege dados, redes, dispositivos, utilizadores e aplicações, garantindo a continuidade do negócio e reforçando a confiança dos seus clientes.

Com a Excelia, a cibersegurança assume-se como um aliado estratégico que permite às empresas operar com segurança, reduzir riscos e cumprir os padrões mais exigentes de proteção da informação, transformando o investimento em cibersegurança num motor de resiliência, confiança e crescimento sustentado.

Fontes

Principais Ciberataques de 2025

Deteção de dados pessoais alegadamente pertencentes à Guardia Civil e ao Ministério da Defesa na dark web. INCIBE. **Ver**

Câmara Municipal de Badajoz restabelece a normalidade após ataque informático. Ayuntamiento de Badajoz **Ver**

Câmara Municipal de Elche sofre ataque informático que deixa o sistema municipal inoperacional. Ayuntamiento de Elche. **Ver**

CNCS acompanha incidente de ransomware notificado pela Agência para a Modernização Administrativa (AMA). Security Magazine. **Ver**

Novo ciberataque ao Ministério do Desenvolvimento Social do Uruguai: mais de 37.000 documentos com dados pessoais divulgados. El País. **Ver**

Município de Porto Nacional (Brasil) alvo de ataque informático que provoca indisponibilidade dos sistemas. Prefeitura Porto Nacional. **Ver**

Publicação oficial da Câmara Municipal de Rio Preto sobre incidente de cibersegurança. Facebook. **Ver**

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

Telefónica investiga alegado ataque informático à Movistar que poderá ter afetado 22 milhões de registos de clientes. RTVE. **Ver**

ING Espanha reconhece incidente de segurança com exposição de dados de clientes. ADSLzone. **Ver**

Comunicado. Santander. **Ver**

Banco Central do Brasil anuncia regras mais rigorosas após aumento dos ciberataques ao sistema financeiro. Reuters. **Ver**

Ciberataque paralisa operações da Jaguar Land Rover. INCIBE. **Ver**

Fraude BEC em multinacional. INCIBE. **Ver**

Relatório de Cibersegurança de 2025

Estatísticas Globais e Tendências de Ataque

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

State of Cybercrime. SentinelOne. **Ver**

Dados Económicos e Custo das Violações de dados

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

Allianz Risk Barometer. Allianz. **Ver**

Análise Regional

Threat Landscape. ENISA. **Ver**

Sucesso da campanha de sensibilização do serviço 017. INCIBE. **Ver**

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

FortiGuard Labs. Fortinet. **Ver**

Previsões Tecnológicas e Estratégia para 2026

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

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

Enquadramento Normativo e Setor Público

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

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

Soluções da Excelia

Cybersecurity Solutions. Excelia. **Ver**

A Excelia é uma multinacional espanhola de consultoria, tecnologia e serviços profissionais, com mais de 25 anos de experiência no mercado. Com escritórios próprios em 9 países e operamos em mais de 50 mercados a nível global. O nosso compromisso é apoiar os clientes na superação dos seus desafios empresariais, promovendo um processo de digitalização contínua, através de soluções e serviços globais impulsionados pela tecnologia.

Trabalhamos para garantir um crescimento sustentável, apostando na inovação e na tecnologia de ponta. Contamos com uma vasta rede de mais de 300 profissionais distribuídos por todo o mundo, uma equipa especializada, global e humana, com conhecimento local e totalmente comprometida com as necessidades de cada cliente

Mais informações em www.excelia.com

nmartins@excelia.com
+351 926 437 847
Avenida da Liberdade, 110 –
1269-046 Lisboa

excelia