Número 108 | Novembro de 2025

NTT DATA

Radar

A sua revista de cibersegurança

NIS2 e DORA: uma estrutura única de governança para a Europa

Por Carlos Chavarría

A União Europeia está caminhando para uma estrutura comum para a cibersegurança. A diretiva NIS2 atualizada e a criação do regulamento DORA buscam unificar a governança de nível executivo, gerenciamento de riscos, gerenciamento de terceiros, gerenciamento de incidentes, cadeia de suprimentos, segurança da informação e continuidade de negócios para criar uma estrutura abrangente.

Essas iniciativas são regulamentadas por setores da União Europeia classificados como críticos na Diretiva NIS2, como energia, transporte, bancos e setor de saúde.

Enquanto isso, o Regulamento DORA padroniza a gestão de riscos de TIC em seguros, mercados de capitais e bancos. Por meio de controles de segurança definidos e padrões técnicos, as ferramentas, métodos, processos e políticas das organizações vêm sendo harmonizadas.

Todas essas mudanças estão aumentando o nível de exigências impostas às empresas e, consequentemente, os custos de conformidade com as regulamentações. De acordo com a IDC, os gastos com cibersegurança devem crescer dois dígitos nos próximos dois anos, com 10,6% em 2023 e 12,3% em 2024, respectivamente.

Espera-se um crescimento próximo dos dois dígitos até 2026, com o mercado europeu girando em torno de US$ 71 bilhões. Paralelamente, o orçamento de TI que as organizações destinam à segurança já chega a 9,0%, segundo a ENISA no relatório emitido para 2024. Como um indicador de intenções de 12 meses, o Relatório de Tendências 2025 da Infosecurity Europe demonstra um aumento médio esperado de 31% nos orçamentos entre os entrevistados.

O aumento de custos é convertido em melhorias nas medidas de segurança das organizações. Esse progresso tem ocorrido tanto em controles preventivos quanto reativos. Atualmente, existe uma conscientização sobre a necessidade de melhorar as medidas de segurança para evitar incidentes.

Ano após ano, o aumento exponencial de ciberataques confirma a importância da implementação de controles reativos e planos de contingência para incidentes e a maneira como eles são relatados. O plano da União Europeia unifica a governança de cibersegurança com a Diretiva NIS2 e o Regulamento DORA na forma de relatar incidentes em tempo hábil.

O NIS2 exige a extensão da governança para além do perímetro, com avaliação contínua de fornecedores, cláusulas contratuais que se estendem aos controles e planos de continuidade compartilhados. A DORA acrescenta um elemento operacional ao setor financeiro: no monitoramento direcionado de provedores críticos de TIC, em cenários de concentração, em testes de resiliência e relatórios sobre incidentes coordenados.

O resultado final é evidenciado por um catálogo exclusivo de requisitos para terceiros, uma matriz de criticidade ativa, com evidências de auditoria consistentes. Ela é gerenciada da mesma forma que a nossa, com due diligence verdadeira: exercícios de crise com fornecedores prioritários, métricas de saúde (com seus respectivos períodos de notificação, cobertura contratual e porcentagem de planos testados) e decisões informadas sobre dependência. O resultado dessa implementação é comprovado por uma quantidade menor de imprevistos, e maior de resiliência mensurável.

A Europa escolheu o modelo a seguir: convergência regulatória, elevando os padrões e medindo rigorosamente o impacto. NIS2 e DORA se complementam. O custo aumenta, mas o retorno também. Isso significa menos tempo de inatividade, menos riscos legais e mais confiança do cliente. Tudo isso é convertido em uma única estrutura de governança NIS2-DORA, um único catálogo de controles para negócios, TI e terceiros, e um relatório de incidente cronometrado que fecha o ciclo. Passamos então da conformidade por obrigação para a demonstração de resiliência através de dados. Embora anteriormente a verificação de caixas fosse usada para demonstrar conformidade, agora a continuidade é protegida.

Carlos Chavarría
Consultor Sênior de Cibersegurança

O *ransomware* não tira férias

Cibercrônica de Antonio Melo e Alejandro Ignacio García

O verão de 2025 demonstrou mais uma vez que o ciberespaço continua preocupante. Enquanto milhões de pessoas ficaram offline, grupos de cibercriminosos e equipes de segurança mantiveram uma luta silenciosa e ininterrupta. O mês de setembro encerrou a temporada de verão, trazendo algumas conclusões realmente preocupantes, combinando ataques de alto impacto, vulnerabilidades críticas e o início de um intenso debate sobre a resiliência de infraestruturas críticas, e uma visão de cibersegurança com inteligência artificial.

Os ataques de *ransomware* mantiveram seu domínio durante os meses de verão. Mais uma vez, os setores de saúde e administração pública foram os favoritos para os ataques de *ransomware*.

Países europeus como Irlanda, Suíça e Alemanha sofreram novamente sequestro de sistema, levando alguns hospitais a cancelar consultas ou adiar operações.

O nível de sofisticação dessas campanhas demonstra como os grupos criminosos mudam sua preferência por táticas híbridas, como dupla extorsão, roubo de informações confidenciais e vazamentos públicos, para pressionar as vítimas.

Zero-days e vulnerabilidades críticas

O verão trouxe consigo vários avisos urgentes dos fabricantes. Vulnerabilidades críticas em sistemas de virtualização ou softwares amplamente implantados em ambientes corporativos forçaram equipes de segurança a aplicar patches em meados de agosto.

A janela de exposição foi reduzida ao extremo mais uma vez, nos lembrando da razão pela qual o ciclo dos patches não é mais medido em semanas, mas em horas.

Geopolítica digital tensa

As tensões internacionais também foram quantificadas no âmbito cibernético.

Este tipo de pesquisa de segurança detectou um aumento significativo em campanhas de espionagem em infraestrutura de energia e transporte na Europa Oriental, vinculadas a atores estatais cujo objetivo é a coleta de inteligência estratégica em um momento dominado pela incerteza geopolítica.

A ascensão ofensiva e defensiva da IA

O mês de setembro consolidou um tema muito debatido: o papel da IA na cibersegurança. À medida que as organizações começam a experimentar algoritmos capazes de detectar anomalias ou até mesmo automatizar a resposta a incidentes, os invasores se esforçam para não ficar para trás: campanhas de *phishing* foram documentadas usando mensagens geradas por IA (que são virtualmente indistinguíveis da comunicação legítima), aumentando o risco para usuários e empresas.

Equilíbrio: um verão que confirma a tendência

A cibercrônica deste verão e de setembro aponta para um padrão claro: a profissionalização do crime digital tem avançado mais rapidamente do que a capacidade de adaptação de muitas organizações.

CISOs e as equipes de segurança devem fortalecer sua capacidade de antecipar *ransomwares*, ataques *zero-days*, campanhas de espionagem, entre outras combinações. O outono está se configurando como um novo capítulo em um tabuleiro onde a única constante é a pressão ininterrupta.

Antônio Melo León
Analista de cibersegurança

Alejandro Ignacio García
Analista Líder em Cibersegurança

GRC: O pilar estratégico da segurança e sustentabilidade organizacional

Artigo de Eduardo Fernando Alves

Em um cenário digital cada vez mais complexo, as organizações enfrentam uma infinidade de riscos que vão muito além das ameaças tecnológicas. A interconexão dos sistemas, a dependência de dados e a constante evolução da legislação exigem uma abordagem integrada à gestão empresarial. É neste cenário que surge o conceito de GRC (Governança, Risco e Conformidade). Trata-se de uma estrutura que permite que as organizações alinhem objetivos estratégicos, gerenciem riscos de forma eficaz e garantam que as operações estejam em conformidade com padrões e regulamentações.

Mais do que um conjunto de processos administrativos, o GRC representa uma filosofia de gestão que combina visão estratégica, disciplina operacional e cultura organizacional. Quando implementado corretamente, ele se torna um verdadeiro diferencial competitivo, promovendo resiliência, transparência e confiança entre todas as partes interessadas.

O que é GRC e por que ele é essencial?

Governança, Risco e Conformidade (GRC) formam um triângulo indissociável dentro das boas práticas corporativas.

A governança define como a organização é administrada, incluindo a estrutura de tomada de decisões, a definição de responsabilidades e o alinhamento com objetivos estratégicos.

A gestão de riscos busca identificar, avaliar e mitigar ameaças que possam comprometer a continuidade do negócio, sejam elas financeiras, operacionais, tecnológicas ou de reputação.

A conformidade garante que todas as atividades organizacionais estejam em conformidade com leis, regulamentos, políticas internas e princípios éticos.

Integrar essas três dimensões é fundamental para garantir que a empresa opere de maneira responsável, transparente e sustentável. Quando o GRC é abordado de forma fragmentada, ele cria um ambiente propenso à ineficiência, retrabalho e falhas que podem causar perdas financeiras, danos à reputação e penalidades legais.

O papel fundamental do GRC na cibersegurança

A cibersegurança transcendeu o âmbito técnico; hoje é uma prioridade estratégica que permeia toda a estrutura organizacional.

Um programa eficaz de Governança, Risco e Conformidade (GRC) fortalece a segurança digital ao estabelecer políticas claras, definir responsabilidades e promover uma cultura de vigilância contínua.

Com o GRC, a empresa pode identificar rapidamente riscos cibernéticos críticos, avaliar o impacto potencial de incidentes e implantar mecanismos robustos de resposta e recuperação.

Esse alinhamento com a estratégia corporativa garante que as decisões sejam tomadas com base em riscos reais, não em percepções.

Além disso, o GRC garante que os controles de segurança não operem isoladamente, mas sejam integrados à auditoria, à conformidade regulatória e ao gerenciamento da continuidade dos negócios. Essa visão holística diferenciará as organizações preparadas para o futuro daquelas que simplesmente reagem às crises.

Cultura e liderança: os fundamentos de um GRC eficaz

Nenhum programa de GRC será eficaz sem o envolvimento e o comprometimento da alta gerência de toda a organização.

A cultura de risco deve ser incentivada de cima para baixo, promovendo comportamento ético, tomada de decisões baseada em evidências e responsabilidade individual. Mais do que documentos e políticas, o GRC é sustentado pelas pessoas e suas atitudes.

A comunicação interna também é um fator determinante. Quando os colaboradores entendem o valor do gerenciamento de riscos e reconhecem seu papel dentro dessa estrutura, o GRC não é mais percebido como um conjunto de obrigações burocráticas, mas como uma ferramenta que dá suporte à tomada de decisões informadas.

Treinamento e conscientização contínuos são igualmente essenciais. Na era da transformação digital, os riscos evoluem diariamente, exigindo que as equipes estejam preparadas para responder com agilidade e critério.

Os benefícios de uma abordagem integrada

A implementação de um modelo GRC maduro traz benefícios significativos para a organização, como:

- Melhor tomada de decisão, baseada em informações consolidadas sobre riscos e controles.
- Redução de custos e duplicação da integração de processos e sistemas de monitoramento.
- Maior confiança de investidores, clientes e reguladores graças à gestão transparente.
- Maior resiliência operacional e capacidade de resposta a incidentes críticos.
- Consolidação da reputação da organização como uma entidade ética, responsável e previsível.

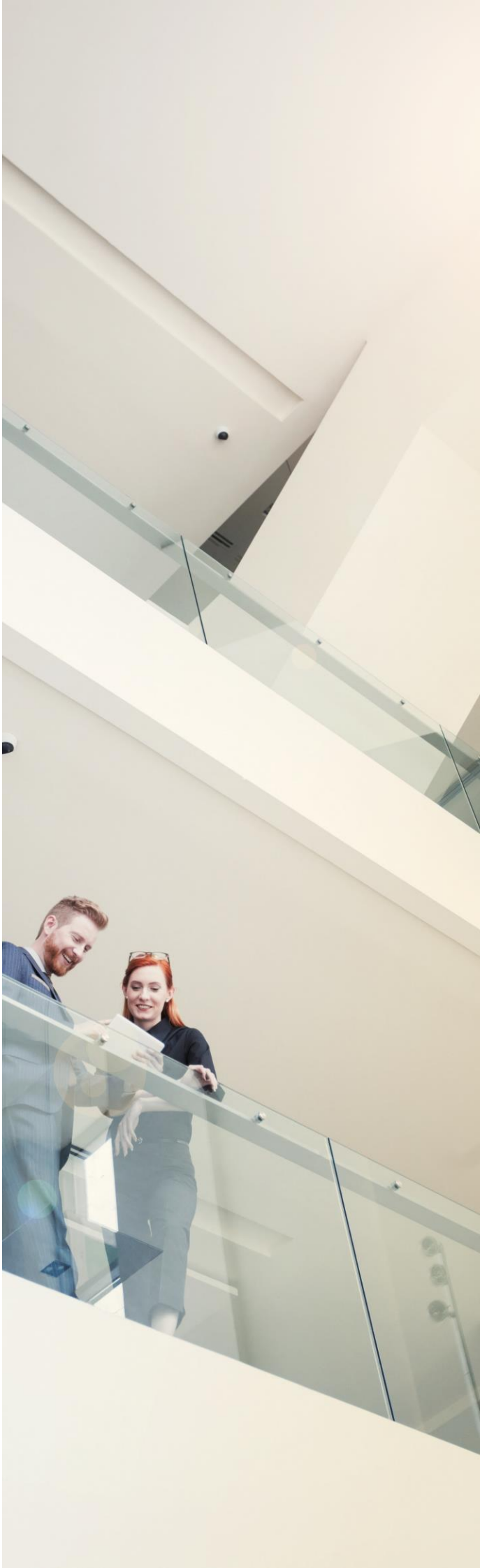
Além desses benefícios tangíveis, o GRC promove a inovação responsável. Ao compreender seus riscos e operar de maneira controlada, a empresa pode explorar novas oportunidades com segurança, sem comprometer a conformidade ou a confiança do mercado.

Os verdadeiros desafios por trás das falhas na implementação do GRC

Apesar de suas promessas, um número significativo de programas de GRC não prosperam. A causa principal? Raramente é uma questão técnica. Na maioria das vezes, o problema está em abordagens desconectadas ou, pior, na falta de comprometimento genuíno da alta gerência.

Outra armadilha comum é a burocracia sufocante. Algumas organizações cometem o erro de adotar estruturas de GRC excessivamente complexas. Em vez de simplificar as operações, elas acabam gerando uma resistência interna generalizada, transformando a conformidade em um obstáculo.

A chave para um GRC verdadeiramente eficaz está na simplificação radical. É fundamental focar no risco real, garantindo que os mecanismos de controle sejam proporcionais e perfeitamente adaptados à realidade da empresa. A tecnologia é uma ferramenta poderosa, capaz de centralizar dados, automatizar relatórios e oferecer rastreabilidade.



No entanto, a ferramenta não deve ser confundida com o objetivo: a tecnologia deve sempre servir à estratégia, nunca o contrário.

O futuro do GRC

Com o avanço da inteligência artificial, automação e análise preditiva, o GRC está entrando em uma nova era.

Ferramentas inteligentes são capazes de identificar padrões de risco, prever incidentes, preparar avaliações de segurança e dar suporte à tomada de decisões em tempo real.

A tendência é que o GRC evolua de uma função de controle reativa para um sistema dinâmico e orientado por dados que antecipa ameaças e orienta os negócios de forma proativa.

Entretanto, à medida que as ferramentas se tornam mais sofisticadas, o mesmo acontece com as responsabilidades éticas e regulatórias. O futuro do GRC exigirá profissionais capazes de equilibrar tecnologia, estratégia e valores humanos, sempre mantendo o foco na integridade e na confiança.

A diferença entre reagir e liderar

Governança, Risco e Conformidade (GRC) não são simplesmente obrigações corporativas. Elas são, de fato, os alicerces que garantem a credibilidade, a segurança e a longevidade de qualquer organização moderna. Vivemos em uma era em que as ameaças cibernéticas estão interconectadas e a pressão regulatória é cada vez maior.

Nesse cenário complexo, o GRC atua como um guia essencial que orienta a liderança a agir de forma responsável e previsível.

Hoje, a maturidade do GRC é o verdadeiro indicador de resiliência. As empresas que adotam esse princípio com rigor e visão estratégica não apenas evitam sanções; elas também constroem ativamente uma base sólida rumo ao crescimento sustentável e, mais importante, conquistam a confiança do futuro.

Eduardo Fernando Alves
Engenheiro Especialista em Cibersegurança

Resiliência operacional digital: risco tecnológico, continuidade do negócio e risco de terceiros

Artigo de Fernando Valles Barbudo

A resiliência operacional digital é uma tendência na gestão de riscos operacionais para todas as empresas. No setor financeiro (bancos e seguros), a regulamentação da Lei de Resiliência Operacional Digital (DORA) entrou em vigor este ano, o que representa mais um passo à frente na gestão e controle de riscos não financeiros. Além disso, pode ser concebido como um compêndio de melhores práticas para empresas não financeiras que, embora não sejam obrigadas a cumprir, desejam repensar seu modelo e cultura de gestão de riscos.

Risco tecnológico

A tecnologia se tornou uma parte altamente relevante das **estratégias de negócios**, deixando de ser vista apenas como um intermédio.

Sua utilização implica automaticamente assumir os **riscos** a ela associados, sendo necessário um **quadro de gestão** adequado e propensão ao risco estabelecida pela Alta Administração. De fato, os riscos da tecnologia da informação e comunicação (TIC) podem se tornar cruciais para a **sobrevivência e resiliência** das empresas.

E não apenas o risco inerente às infraestruturas de TI das próprias entidades é considerado, mas o ecossistema de impacto é muito maior. A tendência de terceirização de infraestrutura para serviços prestados por *hyperscalers,* e sua posição cada vez mais difundida na atividade empresarial como provedores de armazenamento e processamento de operações (na nuvem), faz com que empresas não consideradas entidades financeiras sejam de fato parte do fluxo de análise de risco.

Origens do risco tecnológico

As origens do risco tecnológico são variadas, mas geralmente é utilizada a seguinte classificação:

- **Risco de disponibilidade e continuidade de sistemas**: resulta do impacto adverso no desenvolvimento e na disponibilidade de sistemas e dados de TIC. Isso inclui a falha em recuperar os serviços da entidade em tempo hábil devido a um erro nos componentes de software ou hardware.
- **Risco de segurança da informação:** decorrente do acesso não autorizado aos sistemas e dados de TIC, de dentro ou de fora da instituição.
- **Risco de mudança de sistemas:** resulta da incapacidade da instituição de gerenciar mudanças em seus sistemas de TIC de forma oportuna e controlada.
- **Risco de integridade de dados:** ocorre quando os dados armazenados e processados são incompletos, imprecisos ou inconsistentes em diferentes sistemas, prejudicando a capacidade da instituição de fornecer serviços e gerenciar informações de maneira oportuna e apropriada.
- **Risco de terceirização:** derivados da terceirização de atividades e sistemas. Observe a importância da terceirização da nuvem.

Eventos de qualquer uma dessas fontes podem comprometer a continuidade do negócio.

Risco tecnológico como parte do risco operacional

Risco operacional é definido como o risco de **perdas (econômicas)** decorrentes, entre outras causas, de (i) incidentes no negócio e falhas nos sistemas; (ii) falhas na execução, entrega e gestão de processos; (iii) danos a ativos materiais; ou (iv) fraude (interna ou externa).

Portanto, eventos que geram risco tecnológico devem ser classificados e considerados parte da gestão de risco operacional. Ter uma **gestão integrada** não é uma questão técnica, mas sim uma de governança: **propensão ao risco** única, **taxonomia** comum e **prioridades** alinhadas com o valor do processo e do **negócio**, não apenas com o componente tecnológico em si.

O trinômio processo-risco-controle se estende ao serviço/ativo/plataforma/aplicativo/ vulnerabilidade, e a determinação de risco inerente e residual também é aplicável.

Os perfis de gestão para ambos os tipos de risco são qualitativamente diferentes, mas necessários.

O setor bancário, por exemplo, poderia ser incorporado à estimativa do consumo de capital regulatório para risco operacional.

Processos críticos ou essenciais

Identificar processos críticos é o primeiro passo em qualquer estratégia de resiliência. São aqueles cuja interrupção excede a **tolerância de impacto** comercial. A análise de impacto nos negócios (BIA) deve quantificar as janelas máximas de interrupção (MTPD), o objetivo de tempo de recuperação/objetivo de ponto de recuperação (RTO/RPO) e as dependências: pessoas, dados, aplicativos, infraestrutura e terceiros.

Tenha um **catálogo vivo** de processos essenciais, com seu mapa de processo-ativo-dado-fornecedor e riscos associados quantificados com ou sem mitigadores (riscos inerentes e residuais). Este catálogo **prioriza**, direciona os **testes de resiliência** e alinha todas as **equipes** envolvidas.

Além disso, o mapa de processos deve ser mapeado de forma bilateral com os componentes de TI que dão suporte à operação para identificação e prevenção de riscos: sistemas/processos comprometidos por ataques, vulnerabilidades, falhas diversas, etc.

Processos classificados como críticos devem ser **monitorados** mais de perto, especialmente se houver um terceiro na cadeia de valor.

Testes de continuidade e resiliência do negócio

Nem tudo em continuidade é ISO 22301. No setor bancário, a regulamentação DORA também amplia aspectos relacionados à **continuidade do negócio.**

Além das estratégias proporcionais baseadas no BIA RTO/RPO e no ciclo de melhoria contínua PDCA (*plan-do-check-act*) para o BCM (Business Continuity Management System), vários tipos de **testes de resiliência** são estabelecidos no DORA:

- Avaliações e verificações de vulnerabilidade.
- Análise de código aberto.
- Avaliações de segurança de rede.
- Análise de lacunas (*gap analysis*).
- Revisões de segurança física.
- Questionários e soluções de digitalização automatizada.
- Revisões de código-fonte (quando possível).
- Testes baseados em cenários.
- Testes de compatibilidade e desempenho.
- Testes de ponta a ponta (*end-to-end)*.
- Teste de invasão (*pentesting*).

Risco de terceiros

Os fornecedores são uma parte real da cadeia operacional e digital. Muitos dos problemas têm origem na **terceirização** e em toda a **cadeia de subcontratação**. Portanto, uma boa gestão de riscos de terceiros (TPRM) é essencial e constitui um dos pilares da DORA.

Em termos simples, a gestão de fornecedores deve ser realizada durante todo o **ciclo de vida** do fornecedor: (i) aprovação do fornecedor; (ii) avaliação da relação fornecedor-serviço; (iii) prestação de serviço; e (iv) estratégia de saída.

As **estruturas de controle e auditoria** para operações estão evoluindo, colocando os **processos no centro** e revisando/auditando-os como um todo, independentemente de quem os opera, e incluindo todas as equipes envolvidas nas ações, sejam elas internas ou externas.

Neste ponto, vale a pena fazer algumas **perguntas**: Quantos recursos humanos e técnicos são dedicados à cibersegurança e quantos ao risco de terceiros? Quanto risco real ou potencial se origina na cibersegurança e quanto se origina no risco de terceiros? O investimento dedicado a ambos os blocos é adequado, proporcional e equilibrado em relação ao risco decorrente de cada um? A estrutura de propensão ao risco das empresas é suficientemente detalhada para estabelecer um nível adequado de tolerância, e além disso, identificar os riscos inaceitáveis que devem ser mitigados?

Fernando Valles Barbudo
Diretor de Consultoria Empresarial – Finanças, Risco e Compliance

Internet quântica

Espaço Quântico
por María Gutiérrez

A “internet quântica” é uma nova geração de rede de comunicação que usa as leis da mecânica quântica para transmitir informações.

Se a internet atual se baseia na cópia e transmissão de informações, a internet quântica se baseia em algo muito mais radical: a impossibilidade de copiá-las. Essa ideia, que pode parecer um paradoxo na era da replicação digital, é justamente sua maior força. A base física para isso é o teorema da não clonagem, um dos pilares da mecânica quântica. Este princípio, formulado na década de 1980, afirma que uma cópia exata de um estado quântico desconhecido não pode ser criada. Em outras palavras, se uma partícula carrega informações codificadas em seu estado quântico, por exemplo, a polarização de um fóton, qualquer tentativa de duplicá-la ou medi-la altera irrevogavelmente esse estado. Essa impossibilidade de cópia torna a comunicação quântica, em teoria, protegida de interceptações.

Hoje, a internet quântica é uma realidade em construção. Existem protótipos funcionais e redes experimentais em diferentes partes do mundo. Embora o conceito pareça abstrato, o progresso é real. Em 2017, o satélite chinês Micius demonstrou pela primeira vez a distribuição quântica de chaves entre estações terrestres separadas por 1.200 quilômetros. Na Europa, o projeto EuroQCI está construindo uma rede segura de comunicações quânticas que conectará os Estados-Membros por meio de links terrestres e via satélite. A Espanha participa desta iniciativa por meio do programa Quantum Spain, coordenado pelo Instituto de Ciências Fotônicas (ICFO), o Instituto de Física Teórica (IFT) e o Centro Criptológico Nacional (CCN), que trabalha para adaptar o Marco de Segurança Nacional ao cenário pós-quântico do futuro.

Apesar do progresso, o caminho para uma internet quântica global está repleto de desafios. O primeiro é tecnológico: os qubits são extremamente frágeis e perdem facilmente sua coerência, o que limita sua distância de transmissão. Para resolver esse problema, estão sendo desenvolvidos os chamados repetidores quânticos, que permitiriam estender a rede sem destruir informações. O segundo grande desafio é a infraestrutura. As redes quânticas não substituirão as atuais, mas coexistirão com elas, o que requer protocolos híbridos capazes de integrar com eficiência as comunicações clássicas e quânticas.

Por fim, há um desafio estratégico e geopolítico: as comunicações quânticas têm implicações diretas na segurança nacional e na soberania tecnológica. Os países que dominarem essas redes poderão garantir a confidencialidade de seus dados e proteger sua infraestrutura crítica de futuros ataques de computadores quânticos.

A internet quântica não vai chegar de uma vez só, mas em fases. Veremos primeiro redes quânticas metropolitanas para ambientes financeiros ou governamentais, seguidas pela expansão nacional e, finalmente, pela interconexão global. É possível que, dentro de uma ou duas décadas, o tráfego de informações mais sensível, desde dados médicos até comunicações diplomáticas, ocorra por canais quânticos.

O fascinante dessa revolução é que, quando consolidada, não será visível para o usuário comum. Navegaremos da mesma forma, mas, por baixo da superfície, haverá uma arquitetura completamente nova, projetada não apenas para transmitir informações, mas para preservá-las com um nível de segurança atualmente impossível.

A internet quântica não pretende substituir a atual, mas sim complementá-la. Enquanto as redes tradicionais se baseiam no eletromagnetismo clássico e na criptografia matemática, a rede quântica se baseia nas leis fundamentais da natureza. Não será apenas uma evolução tecnológica, mas uma nova maneira de entender a comunicação, assim, a proteção de dados não dependerá mais de algoritmos e será incorporada às próprias leis da física.

Gestão de riscos de terceiros

Tendências por Antonio Chavarría

De acordo com o último Relatório de Investigações de Violações de Dados da Verizon, até 2025, 89% das violações de segurança terão origem em vulnerabilidades de terceiros. Essa estatística não é apenas um número: ela representa a realidade de que o perímetro de segurança tradicional desapareceu. As organizações modernas operam em ecossistemas digitais complexos, em que o número médio de fornecedores críticos por empresa cresceu 340% nos últimos três anos, transformando o gerenciamento de riscos de terceiros (TPRM) de uma função administrativa em um imperativo estratégico para a sobrevivência dos negócios.

A convergência da inteligência artificial, regulamentações como NIS2 e DORA e a profissionalização de grupos como o Scattered Spider criaram um cenário em que os métodos tradicionais de avaliação de fornecedores são tão eficazes quanto uma armadura medieval contra um ataque cibernético moderno.

Revolução do monitoramento contínuo

O paradigma das avaliações anuais ou semestrais entrou em colapso diante da velocidade exponencial com que as ameaças evoluem. Grupos como APT40 e Lazarus podem comprometer um fornecedor e migrar para alvos secundários em menos de 72 horas, enquanto avaliações tradicionais levam de 45 a 90 dias para serem concluídas.

Organizações líderes adotaram sistemas de monitoramento contínuo 24 horas por dia, 7 dias por semana, que combinam:

- Gerenciamento de Superfície de Ataque Externa (EASM): Plataformas como Recorded Future e RiskIQ verificam automaticamente ativos de fornecedores externos, identificando:
  - Vulnerabilidades críticas dentro de 4 horas após a publicação.
  - Certificados SSL expostos ou mal configurados.
  - Serviços de TI paralelos não documentados.
  - Exposição acidental de banco de dados (mais de 23.000 bancos de dados MongoDB foram encontrados expostos em 2024).

- Threat Intelligence contextualizada: integração com feeds Mandiant, CrowdStrike e Microsoft Defender que alertam sobre:
  - Menções de fornecedores em fóruns de *ransomware*, como o LockBit 3.0.
  - Atividade suspeita na *dark web* relacionada a credenciais corporativas.
  - Campanhas de *phishing* que visam especificamente ecossistemas de fornecedores.

- Análise comportamental com IA: Algoritmos de *machine learning* que estabelecem linhas de base comportamentais para cada fornecedor, detectando desvios como:
  - Comportamentos de acesso anormais em sistemas críticos.
  - Alterações não documentadas na infraestrutura de rede.
  - Aumentos repentinos na transferência de dados.

Inteligência artificial, o motor da transformação do TPRM

A inteligência artificial está revolucionando todos os aspectos do ciclo de vida do TPRM. Os sistemas de IA generativa são capazes de analisar contratos de fornecedores, relatórios SOC 2 e documentação técnica em minutos (em vez de horas). O processamento de linguagem natural identifica automaticamente cláusulas de risco, lacunas de responsabilidade e obrigações de conformidade.

Recursos mais avançados incluem:

- Geração automática de questionários: sistemas que criam avaliações personalizadas com base no perfil de risco específico de cada fornecedor, o tipo de serviço prestado e as regulamentações aplicáveis.
- Análise preditiva de riscos: modelos de *machine learning* que combinam dados históricos, tendências do setor e IA para prever a probabilidade de ameaças de segurança.
- Automação de resposta: agentes de IA que podem gerar rascunhos de planos de remediação, correspondências com fornecedores e relatórios executivos baseados em resultados de avaliações.

Conformidade dinâmica e adaptativa

A tecnologia regulatória (RegTech) está transformando a maneira como as organizações gerenciam a conformidade regulatória em seus relacionamentos com terceiros.

Os sistemas RegTech são capazes de rastrear mudanças regulatórias em tempo real e avaliar automaticamente seu impacto no relacionamento com fornecedores, oferecendo:

- Monitoramento regulatório contínuo: sistemas que rastreiam automaticamente mudanças em regulamentações como GDPR, DORA e NIS2 e avaliam o impacto em contratos e processos existentes.
- Avaliações KYC/AML automatizadas: processos totalmente automatizados para verificação de identidade, detecção de lavagem de dinheiro e triagem de listas de sanções.
- Relatórios de conformidade automáticos: ferramentas que geram automaticamente relatórios regulatórios com validação de dados integrada e formatação de acordo com padrões específicos.

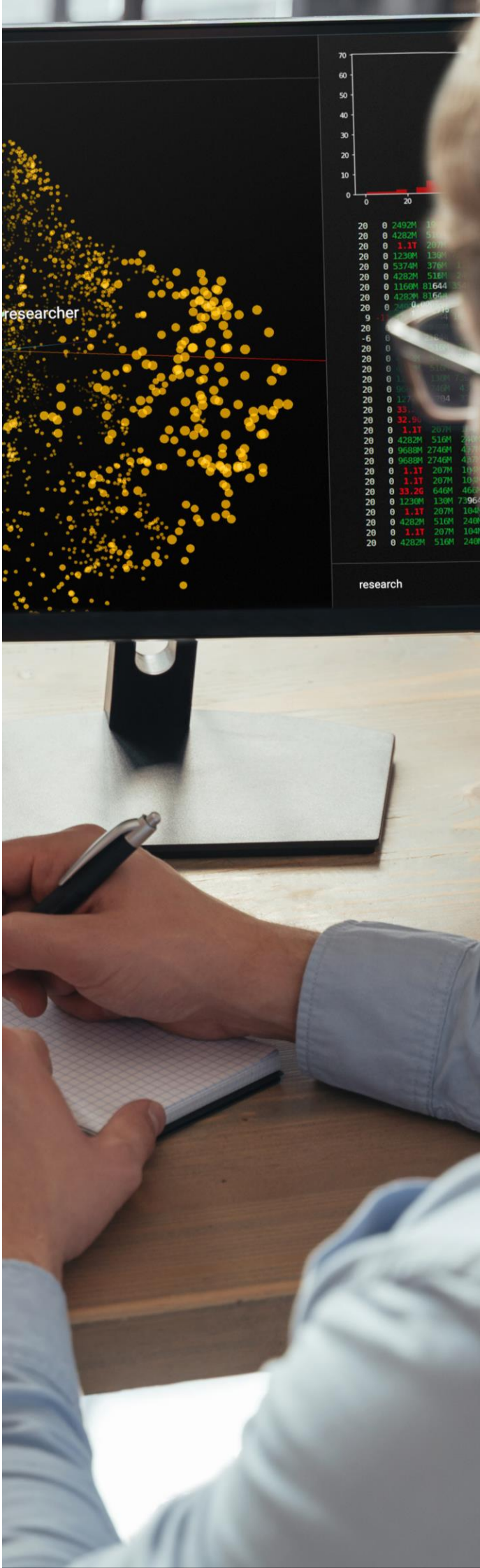
Futuro do TPRM

O gerenciamento de riscos de terceiros tem evoluído para ecossistemas inteligentes que combinam IA, automação e análise preditiva para criar recursos de gerenciamento de riscos sem precedentes. Organizações que adotarem essas tecnologias emergentes não apenas melhorarão sua postura de segurança, mas também ganharão vantagens competitivas significativas em um mundo cada vez mais interconectado.

O sucesso dessa transformação exige mais do que uma implementação tecnológica: requer uma mudança cultural em direção à colaboração proativa com fornecedores, investimento em capacidades analíticas avançadas e comprometimento executivo com a excelência na gestão de riscos.

As organizações que lideram essa evolução definirão o futuro dos ecossistemas de negócios digitais.

Antonio Chavarría
Consultor Sênior de Cibersegurança



Golpes de APP no Reino Unido e seus requisitos de reembolso obrigatório

Artigo de Octavio Sánchez Blanco

O Reino Unido assumiu a liderança em sua cruzada contra fraudes e, há alguns meses, aprovou uma regulamentação em que, em determinadas circunstâncias, os provedores de serviços de pagamento serão obrigados a reembolsar valores roubados. Neste artigo analisamos as implicações desta regulamentação.

Todos os anos, milhares de pessoas e empresas são vítimas de golpes. Neste artigo, abordamos aqueles que preocupam especialmente o setor bancário, devido ao alto custo reputacional e aumento, tanto em número quanto em quantidade, observado nos últimos anos. Esses são chamados de *Authorised Push Payment Scams,* golpes de pagamento por push autorizado (APP).

Esse tipo de golpe ocorre quando a vítima é enganada e envia dinheiro para um golpista que se passa por um destinatário genuíno.

Existem muitos modus operandi para enganar as vítimas, mas podemos resumi-los em dois grandes grupos: "destinatário malicioso" e "redirecionamento malicioso".

No primeiro caso, o golpista faz com que a vítima compre um bem ou serviço que não existe ou que nunca será entregue; no segundo, o golpista se passa por um banco ou prestador de serviço técnico (empresa de gás, água ou tecnologia) para enganar a vítima e fazê-la transferir dinheiro de sua conta bancária para uma conta controlada pelo golpista.

Recentemente, o Reino Unido assumiu a liderança no combate a esse tipo de golpe, sendo pioneiro na adoção de regulamentações de reembolso obrigatório para golpes de pagamento por push autorizados (APP), que entraram em vigor em 7 de outubro de 2024.

Anunciadas pelo Regulador de Serviços de Pagamento (PSR) em 7 de junho de 2023, as novas regras exigem que os provedores de serviços de pagamento do Reino Unido reembolsem todos os clientes que forem vítimas de golpes de APP, com exceções limitadas.

No Reino Unido, o valor de fraudes de pagamento autorizados atingiu £ 459,7 milhões em 2023, com um total de 232.429 casos. O reembolso total às vítimas foi de £ 287,3 milhões, representando 62% do total de perdas relatadas (gráfico no final da página).

- Cases (Casos): número de casos confirmados relatados. Um caso é igual a uma conta, não a um indivíduo.
- Payments (Pagamentos): número total de pagamentos identificados como fraudulentos em relação aos casos relatados.
- Value (Valor): valor total dos pagamentos relatados.
- Returned to victim (Devolvido à vítima): valor total devolvido à vítima, seja porque o banco emitiu o reembolso diretamente ou porque o valor foi recuperado da conta do beneficiário.

		2020	2021	2022	2023	CHANGE
CASES	PERSONAL	145,207	188,964	200,643	224,694	12%
	NON-PERSONAL	9,407	7,032	6,729	7,735	15%
	TOTAL	154,614	195,996	207,372	232,429	12%
PAYMENTS	PERSONAL	228,946	333,751	361,761	405,095	12%
	NON-PERSONAL	15,625	11,386	10,505	12,364	18%
	TOTAL	244,571	354,137	372,266	417,459	12%
VALUE	PERSONAL	£347.4m	£505.9m	£408.2m	£376.4m	-8%
	NON-PERSONAL	£73.3m	£77.4m	£77.0m	£83.3m	8%
	TOTAL	£420.7m	£583.2m	£485.2m	£459.7m	-5%
RETURNED TO VICTIM	PERSONAL	£163.4m	£246.8m	£254.1m	£256.4m	1%
	NON-PERSONAL	£27.4m	£24.4m	£31.5m	£30.8m	-2%
	TOTAL	£190.8m	£271.2m	£285.6m	£287.3m	1%

Fonte: Relatório Anual de Fraude 2024. UK Finance

Em termos gerais, os objetivos desta implementação no Reino Unido são:

- Incentivar o investimento do setor na prevenção de fraudes de ponta a ponta.
- Aperfeiçoar a proteção ao cliente e a confiança no ecossistema de pagamentos.
- Cumprir o objetivo de longo prazo do PSR, fazendo com que o órgão de padronização de sistemas de pagamentos interbancários do Reino Unido (Pay.UK) assuma um papel mais amplo e melhore ativamente as regras para pagamentos mais rápidos.

Os novos requisitos provocarão uma mudança radical na cultura de pagamento para melhorar a prevenção de fraudes e concentrar todos os esforços das empresas na proteção dos clientes.

Aspectos acordados

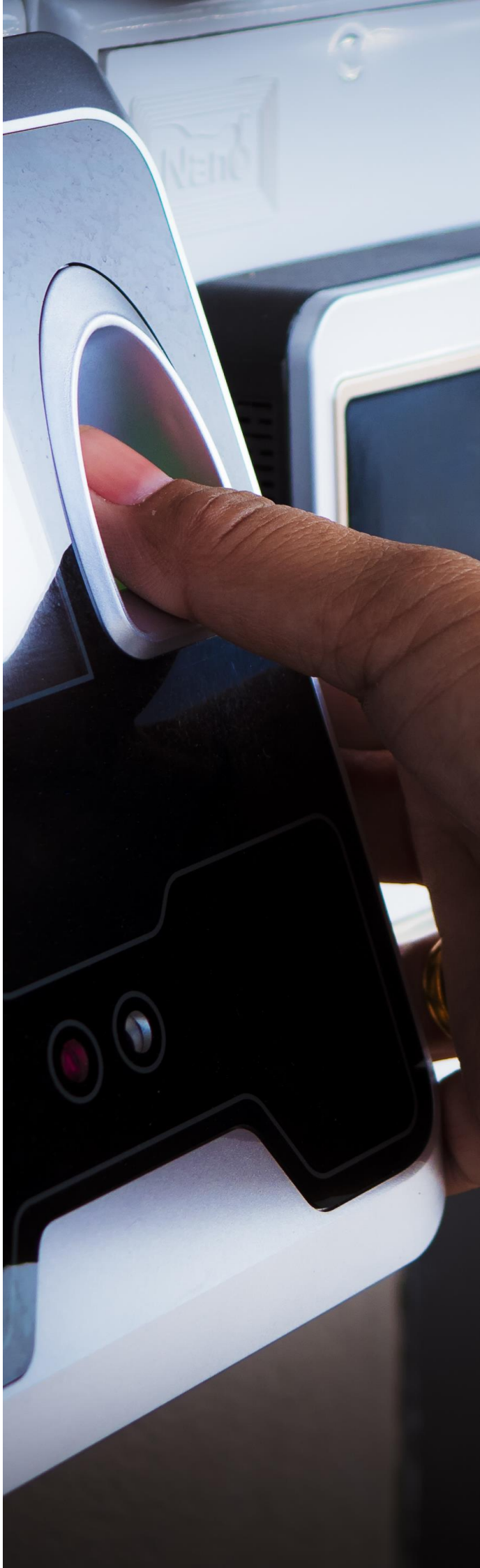
Essas regras são obrigatórias para todos os provedores de serviços de pagamento (PSPs) que usam o sistema Faster Payments, abrangendo praticamente todos os golpes de APP.

As decisões relacionadas a reembolso são tomadas exclusivamente pelo PSP emissor. No entanto, este pode reivindicar 50% de qualquer reembolso do fornecedor de serviços de pagamento.

O PSP deve emitir o reembolso no prazo de cinco dias úteis, embora possa estender esse prazo caso precise realizar investigações (até, no máximo, 35 dias).

Um valor máximo de reembolso de £ 415.000 foi proposto inicialmente, mas foi reduzido para £ 85.000 pouco antes da data de início dessas medidas. O regulador justificou essa mudança como um ajuste prático para evitar possíveis abusos do sistema, enfatizando que esse novo limite cobriria mais de 99% dos casos de fraude.

Os novos requisitos introduzem o "padrão de precaução do consumidor", que estabelece exceções a essa obrigação geral de reembolso: quando o consumidor que solicita o reembolso agiu de forma fraudulenta e/ou com negligência grave. É claro que o “padrão de precaução do consumidor” não se aplicaria a consumidores identificados como vulneráveis a um golpe de APP.



Um reembolso só pode ser negado se o cliente não tiver cumprido o "padrão de precaução do consumidor" pelos motivos descritos acima e somente se o cliente não for considerado vulnerável. Além disso, o Regulador de Pagamentos do Reino Unido (PSR) se compromete a:

- Divulgar regularmente o nível de proteção que as empresas oferecem aos seus clientes.
- Configurar a “Confirmação do Beneficiário” (VoP, um sistema de verificação de nome para pagamentos para ajudar a evitar golpes e pagamentos mal direcionados).
- Promover melhor compartilhamento de inteligência entre empresas de pagamento para detectar transações fraudulentas e evitar que elas ocorram.

As reivindicações podem ser feitas em até 13 meses (embora os PSPs possam optar voluntariamente por conceder reembolsos para reivindicações subsequentes).

Em resumo, o Reino Unido está tomando medidas para garantir a proteção do consumidor contra a crescente ameaça de golpes de pagamento autorizados (golpes de APP), adaptando-se à implementação da PSD3, cujo rascunho exige atenção especial aos clientes particularmente vulneráveis.

Ao garantir o reembolso para esses tipos de casos de fraude, o regulador britânico (PSR) pretende forçar as instituições a tomarem a iniciativa de prevenir essas técnicas ilícitas. A colaboração entre organizações e com empresas de telecomunicações é essencial, assim como a inclusão de novas tecnologias, como a biometria comportamental, para melhorar a detecção e a mitigação desses golpes, que acabam causando danos à reputação.

O Reino Unido foi pioneiro com a nova regulamentação. Organizações em outros países precisarão prestar atenção ao impacto dessas regulamentações sobre os reguladores nacionais.

O regulador planeja publicar um relatório no segundo trimestre de 2026. Este documento refletirá os resultados de uma avaliação independente do impacto das políticas implementadas em relação aos golpes de APP, incluindo as regras de reembolso discutidas neste artigo. Para tanto, será analisada a eficácia e o cumprimento de cada política, bem como o tratamento de casos de fraude envolvendo clientes vulneráveis.

Octavio Sánchez Blanco
Líder de FinCrime do FRC

Fontes:

Site do regulador do Reino Unido resumindo todo o trabalho da agência sobre golpes de APP (https://www.psr.org.uk/our-work/app-scams/)
Documento elaborado pelo regulador britânico (PSR) sobre o conceito de “padrão de precaução do consumidor". (https://www.psr.org.uk/media/as3a0xan/ sr1-consumer-standard-of-caution-guidance-dec-2023.pdf)
Documento elaborado pelo regulador do Reino Unido (PSR) sobre políticas de combate a golpes de pagamento por push autorizados (golpes de APP). (https://www.psr.org.uk/ media/kwlgyzti/ps23-4-app-scams-policy-statement- dec-2023.pdf)

Golpes: o que são e quais os tipos mais comuns?

Artigo de Octavio Sánchez Blanco

A quantidade de golpes aumentou significativamente nos últimos anos, criando uma sensação de insegurança em toda a população, que se sente ameaçada pelos cibercriminosos. Neste artigo, explicaremos o que é um golpe, os tipos mais comuns e como evoluem.

Um golpe é um ato fraudulento em que uma pessoa engana outra com a intenção de obter benefício, principalmente econômico. Normalmente, quando um golpe é realizado, informações falsas são usadas para manipular a vítima e fazê-la tomar decisões que, normalmente, não tomaria. Golpes podem ocorrer de diversas maneiras e métodos, desde simples até esquemas complexos.

É necessário diferenciar golpe e fraude. Enquanto neste último caso é o fraudador que utiliza diversas técnicas para obter os dados necessários e cometer fraude econômica, no golpe é a própria vítima quem realiza a transação. Vale ressaltar que, em caso de fraude, a vítima não é tão protegida.

Tipos mais comuns

Golpes de caridade, loteria ou prêmios

Golpistas fingem representar uma instituição de caridade (legítima ou falsa) e solicitam doações em situações de desastres naturais ou outras emergências, por exemplo, quando há uma guerra.

Em outros casos, os golpistas informam que a vítima ganhou um prêmio de loteria ou sorteio, solicitando um pagamento adiantado para cobrir taxas ou impostos sobre a suposta recompensa a ser recebida. Na era digital, os avanços tecnológicos, o uso e a dependência da tecnologia levaram à evolução e diversificação dos golpes, tornando tanto indivíduos quanto grandes organizações alvos claros.

Na Espanha, a fraude online é o tipo de crime que mais cresce, aumentando 509,1% entre 2016 e 2023. No primeiro trimestre de 2024, um em cada sete crimes se enquadrava nessa categoria.

Golpes de emprego falso

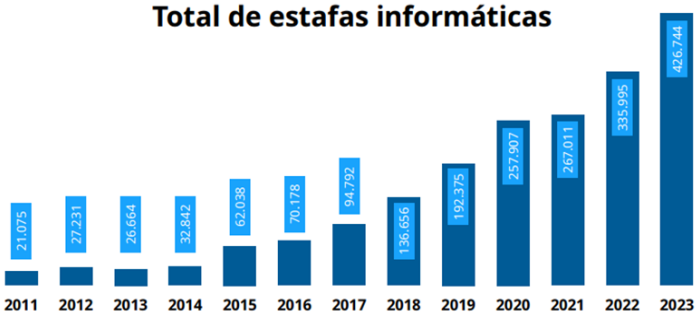
Hoje em dia, tentativas de golpes de emprego via WhatsApp ou LinkedIn são muito comuns. Os criminosos fingem trabalhar no departamento de Recursos Humanos ou Administrativo de uma empresa ou negócio conhecido. Eles costumam oferecer home office, atividades que exigem pouco esforço e tempo, com muita flexibilidade e boa remuneração.

Eles então pedem taxas administrativas para enviar equipamentos de trabalho, ou alguma outra desculpa para que a vítima realize um pagamento adiantado pelo trabalho a ser executado.

Golpes de investimento

Golpes de investimento são um dos tipos mais comuns atualmente, devido ao crescimento das mídias sociais e plataformas ou aplicativos de investimento on-line, onde golpistas encontraram novas maneiras de atingir um grande número de vítimas em potencial, com promessas de riqueza instantânea ou altos retornos de investimento.

Os golpistas usam uma variedade de estratégias, além de prometer grandes lucros, como esquemas Ponzi, em que pagam os rendimentos dos investidores anteriores com o dinheiro dos novos, ou esquemas de pirâmide, onde incentivam a recrutar mais pessoas para manter os lucros fluindo, assim, a falha no recrutamento faz com que a vítima não receba seus rendimentos.



Balance de Criminalidad del Ministerio del Interior

Frequentemente, solicitam que a vítima instale um aplicativo de controle remoto, como o AnyDesk, em seus dispositivos, sob o pretexto de ensiná-la a realizar transações de investimento. Os dispositivos de acesso são controlados e transações fraudulentas realizadas sem o conhecimento da vítima. Para perfis de investimento específicos, golpes relacionados a esquemas de *pump-and-dump* (inflação artificial do preço de uma ação ou ativo por meio de informações falsas), opções binárias, microcaps ou seminários sobre investimentos são comuns.

OS 5 MAIORES GOLPES DE INVESTIMENTO

- Esquema Ponzi
- Esquemas de bombeamento e despejo
- Esquemas de pirâmide
- Fraude de taxa antecipada
- Golpes de opções

Investimentos em criptomoedas ou golpes de grupos de afinidade (por exemplo, investimentos em Forex) merecem atenção especial devido ao crescimento exponencial.

Golpes de suporte técnico

Também conhecido como golpe da Microsoft, ele explora a ignorância tecnológica de certos setores da população. Golpistas usam engenharia social para solicitar informações pessoais e confidenciais da vítima, usando ligações ou e-mails para alertar sobre um problema de segurança no dispositivo, que requer intervenção imediata para evitar problemas futuros. Com tais informações em mãos, eles usam engenharia social para conceder acesso remoto ao dispositivo.

Golpes comerciais

Um dos golpes mais antigos, usado desde que transações comerciais de qualquer tipo passaram a existir. Hoje em dia, elas podem ocorrer por meio de sites de comércio eletrônico não seguros e sites de leilão, são muito comuns nas mídias sociais e, especialmente recentemente, em aplicativos de varejo online como Wallapop ou Vinted.

São anúncios falsos nos quais a vítima faz pagamentos antecipados por bens ou serviços que nunca receberá ou que não existem. Os produtos e/ou serviços para esse tipo de golpe são muito variados e podem mudar dependendo da época do ano.

Podem ser anúncios de aluguel de férias, pellets (combustível para sistemas de aquecimento), carros, adoção de animais de estimação e muito mais.

Golpes românticos

Golpistas usam plataformas como mídias sociais ou aplicativos/sites de namoro para criar perfis atraentes usando fotos e bios falsas para atrair vítimas em potencial. Às vezes, eles até “personificam” artistas conhecidos ou pessoas renomadas. É muito comum que se passem por militares no exterior.

É um tipo de golpe que tende a durar muito tempo, estabelecendo uma forte conexão emocional com a vítima por meio de comunicação frequente, demonstrações de afeto e interesse “genuíno” em sua vida.

Depois de conquistarem a confiança da vítima, eles geralmente alegam algum tipo de problema de saúde, emergência financeira, custos de viagem ou problemas de visto para se encontrarem pessoalmente. Eles tentam pressionar a vítima com falsas emergências e fazem com que ela, emocionalmente envolvida, não considere a natureza da situação.

É alarmante como algumas vítimas podem perder grandes quantias, às vezes todas as economias, além de sofrerem grave sofrimento emocional, vergonha e humilhação, aumentando a solidão e o isolamento.

Golpes que se fazem passar por uma agência oficial ou empresa de serviços

O golpista se passa por uma dessas organizações através de ligações, e-mails ou mensagens de texto alertando sobre uma suposta dívida com a Receita Federal, ou com a empresa, ameaçando um corte imediato de energia ou água, um pacote que não será entregue e solicitando pagamentos diretos da vítima.

Golpes de manipulação de IBAN/fraude de fatura

É um tipo de golpe mais comumente direcionado a empresas, embora pessoas físicas também possam ser vítimas. Os golpistas utilizam técnicas de engenharia social para obter os dados ou endereços de e-mail de um fornecedor ou prestador de serviços regular de uma empresa e, em seguida, interceptam ou manipulam uma fatura digital ou física para alterar as informações da conta e garantir que a próxima transação bancária seja direcionada para suas próprias contas.

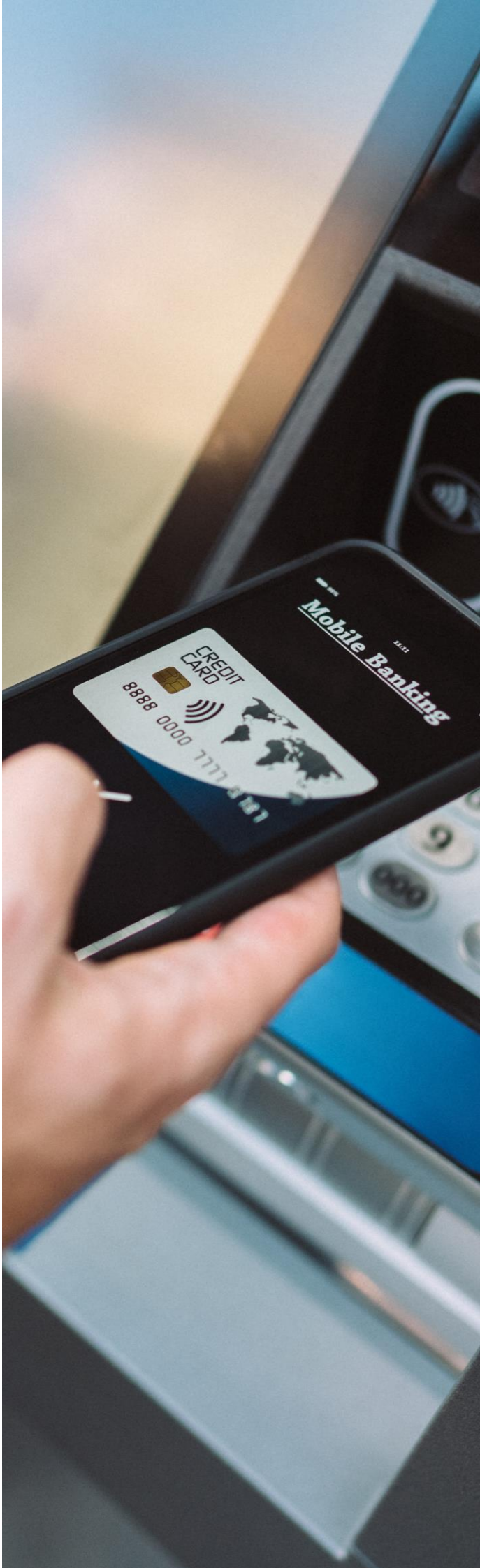
Normalmente, o valor e o prazo são consistentes com transações anteriores com a empresa que foi falsificada.

Golpes de falsificação de identidade bancária

A personificação de um funcionário bancário é um tipo crescente de golpe. Eles geralmente entram em contato por telefone e podem já ter algumas informações sobre a vítima, obtidas por meio de outras estratégias de engenharia social.

Eles se apresentam como gerentes ou membros dos departamentos de segurança, como um funcionário de verdade faria. Eles informam a vítima sobre algum tipo de atividade suspeita em suas contas ou sobre uma transação que o cliente não autorizou, gerando ansiedade, urgência e preocupação na vítima. Sob o pretexto de tomar medidas imediatas para proteger seu dinheiro, são persuadidos a fornecer os dados de login do banco on-line, compartilhar informações de autenticação de dois fatores para confirmar transações, ou fazer transações diretamente para a conta do golpista.

Técnicas conhecidas como *spoofing* são frequentemente usadas para fazer com que as chamadas pareçam vir de números de telefone oficiais dessas entidades, como o Atendimento ao Cliente.



Golpes de representação de membros da família

Muito comum via WhatsApp, esse tipo de golpe disparou nos últimos anos. Geralmente surgem, por exemplo, de uma criança que está estudando no exterior ou viajando no momento e relata uma situação de emergência repentina que a obriga a escrever de um número desconhecido. Às vezes, eles usam informações específicas sobre o filho da vítima que podem encontrar nas redes sociais.

Apelando para as preocupações da família, eles continuam enfatizando a natureza crítica da situação e que um atraso no valor solicitado terá consequências sérias para eles. Exigem transferências de dinheiro imediatas, impossíveis de interromper quando a vítima percebe o golpe.

Golpe de recrutamento de laranjas

Eles começam de forma semelhante aos golpes de emprego falso. Golpistas anunciam empregos legítimos ou contatam pessoas diretamente pelas redes sociais, com o benefício adicional de convencê-las a agir como agentes, ou seja, a criar uma conta bancária para esse propósito ou usar a sua própria para transferir dinheiro que acreditam ser legítimo. Em muitos casos, as vítimas não têm consciência do crime que estão cometendo.

A rede de laranjas facilitará a lavagem de dinheiro de outros golpes ou fraudes por meio de pagamentos em tempo real, transferindo valores rapidamente entre várias contas.

Fraude de CEO

Nesse tipo de golpe, um criminoso ou um grupo de criminosos, usando diversas técnicas de engenharia social, consegue se passar pelo CEO de uma empresa. O modus operandi consiste em convencer um responsável pelas contas ou transações da empresa a fazer transferências urgentes para a conta do golpista.

É um tipo de golpe que comumente afeta empresas e normalmente é realizado por meio de canais como WhatsApp, SMS ou chats usados pela empresa, como o Microsoft Teams.

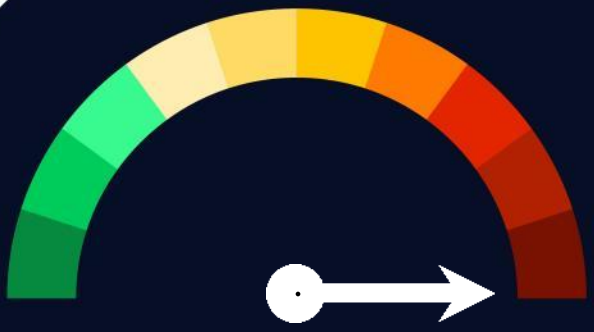
Como vimos, a gama de tipos de golpes é muito ampla e está em constante evolução. Por isso, o desafio imposto por esse crescimento exponencial, tanto em termos de tipo quanto de número de ataques, exige investimento constante em recursos que facilitem a proteção ao consumidor. Além disso, é necessária uma gestão adequada de prevenção de fraudes e mitigação de quaisquer penalidades que possam surgir devido à regulamentação.

Diego José de Benito
Analista de FinCrime
Risco Financeiro e
Compliance (FRC)

Vulnerabilidades

Vulnerabilidade crítica no Redis

Data: 3 de outubro de 2025
CVE: CVE-2025-49844



CVSS: 9.9

CRÍTICA

Descrição

A vulnerabilidade **CVE-2025-49844** (chamada de "RediShell") representa uma ameaça crítica, permitindo que invasores executem códigos remotamente em milhares de instâncias vulneráveis.

Esta é uma falha de uso após liberação (CWE-416) que está presente no código-fonte do Redis há mais de uma década. Assim, um invasor com credenciais válidas poderia usar um script Lua especialmente criado (um recurso habilitado por uma falha) para escapar do *sandbox* (ambiente seguro), acionar o erro de memória, estabelecer uma conexão reversa persistente (*reverse shell*) e, por fim, executar o código remoto no sistema afetado.

Solução

O Redis recomenda **atualizar para a versão 8.2.2**, especialmente para instâncias acessíveis pela Internet:

- Uma solução alternativa adicional para atenuar o problema sem corrigir o executável redis-server é impedir que os usuários executem scripts Lua. Isso pode ser feito usando ACLs para restringir os comandos EVAL e EVALSHA.

Produtos afetados

Essa vulnerabilidade crítica afeta as **versões 8.2.1 e anteriores**, permitindo que um usuário autenticado use um script Lua especialmente criado para manipular o coletor de lixo, acionando o uso após liberação e, potencialmente, levando à execução remota de código.

Referências

- nvd.nist.gov
- bleepingcomputer.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidade crítica no Flag Forge

Data: 10 de outubro de 2025
CVE: CVE-2025-617777

CVSS: 9.4

CRÍTICA

Descrição

Uma vulnerabilidade crítica foi identificada no Flag Forge, uma plataforma usada para competições Capture The Flag (CTF).

A falha foi encontrada nos endpoints administrativos */api/admin/badge-templates* (GET) e */api/admin/badge-templates/create* (POST), que permitiam acesso sem autenticação ou autorização.

Essa vulnerabilidade, com uma pontuação CVSS de 9,4, pode ser explorada por um invasor remoto não autenticado para obter todos os modelos de crachás contendo dados confidenciais, bem como criar modelos arbitrários diretamente no banco de dados.

Solução

É recomendável atualizar imediatamente para a versão 2.3.2, na qual a vulnerabilidade já foi corrigida.

Produtos afetados

A vulnerabilidade afeta os seguintes produtos:
Plataforma Forge CTF: versão 2.0.0 a 2.3.1

Referências

- incibe.es
- github.com

TLP:WHITE

Oracle corrige vulnerabilidade *zero-day* no Oracle E-Business Suite

Data: 5 de outubro de 2025
CVE: CVE-2025-61882

Crítica

Descrição

A Oracle lançou um patch urgente para uma vulnerabilidade *zero-day* em seu E-Business Suite (EBS), identificada como **CVE-2025-61882**, que tem sido usada ativamente pelo grupo Clop em ataques de roubo de dados.

Segundo a Oracle, essa fraqueza está no componente "Integração do BI Publisher" do módulo "Processamento Simultâneo" do EBS.

O pior é que ele não requer autenticação: um invasor pode executá-lo pela rede sem nome de usuário ou senha, permitindo a execução do código remotamente se a exploração for bem-sucedida.

A vulnerabilidade tem uma pontuação base CVSS de **9,8**, refletindo sua criticidade, dada a facilidade com que pode ser explorada e seu impacto potencial.

Produtos afetados

A Oracle confirmou que a vulnerabilidade *zero-day* afeta o produto Oracle E-Business Suite, da versão 12.2.3 até a versão 12.2.14.

Solução

A Oracle lançou uma atualização de emergência para corrigir a falha, embora a Atualização Crítica de Patch de outubro de 2023 deva ser aplicada primeiro para instalar o patch de emergência contra o CVE-2025-61882.

Referências

- nvd.nist.gov
- bleepingcomputer.com

IBM corrige vulnerabilidades que permitem escalonamento de privilégios

Data: 9 de outubro de 2025
CVE: CVE-2025-36356 e mais 2

Crítica

Descrição

A IBM lançou um boletim de segurança para abordar diversas vulnerabilidades nos produtos IBM Security Verify Access e IBM Verify Identity Access.

O mais grave (CVE-2025-36356) permitiu que um usuário autenticado localmente elevasse seus privilégios ao nível raiz ao executar com mais permissões do que o necessário. Esta vulnerabilidade tem uma pontuação CVSS de 9,3.

Além disso, outros bugs que poderiam permitir a execução não autorizada de comandos ou a inclusão de código de ambientes externos foram corrigidos.

Produtos afetados

Os produtos afetados pela atualização são os seguintes:

- IBM Security Verify Access (Docker e Appliance): versões 10.0.0.0 a 10.0.9.0-IF2
- IBM Verify Identity Access (Docker e Appliance): versões 11.0.0.0 a 11.0.1.0

Solução

A IBM recomenda atualizar os produtos afetados para as versões corrigidas:

- IBM Security Verify Access: aplicar Fix Pack 10.0.9.0-IF3
- IBM Verify Identity Access: aplicar Fix Pack 11.0.1.0-IF1

Referências

- ibm.com
- incibe.es

TLP:WHITE

Eventos

19ª Conferência STIC CCN-CERT | 7ª Conferência ESPDEF-CERT de Defesa Cibernética | Congresso RootedCON

24 a 27 de novembro

O maior evento nacional de cibersegurança será realizado no cinema Kinépolis Ciudad de la Imagen, em Madri, com o tema "Um escudo digital para uma Espanha interconectada". Pela primeira vez, o National Cryptologic Center (CCN), o Joint Cyberspace Command (MCCE) e a RootedCON estão unindo forças para criar um programa integrado que reunirá mais de 7.000 profissionais.

O evento começará em 24 de novembro com uma edição especial da conferência RootedCON focada em treinamento e sessões práticas. As principais sessões ocorrerão de 25 a 27 de novembro, destacando as últimas pesquisas, políticas e tecnologias de cibersegurança.

Link

Reuniões de TI e Cibersegurança em Marbella

18 a 20 de novembro

Uma feira inovadora dedicada a soluções de rede, nuvem, mobilidade, cibersegurança e IA será realizada no Centro de Conferências de Marbella (Málaga). O evento utiliza um conceito exclusivo de reuniões de negócios pré-agendadas de 15 minutos entre tomadores de decisão qualificados da França, Itália, Alemanha e Suíça e expositores internacionais.

A feira reunirá mais de 80 expositores e 150 tomadores de decisão, com oportunidades de networking por meio de jantares-coquetéis que permitirão o desenvolvimento contínuo de negócios em um ambiente descontraído.

Link

Fórum ISMS Espanha

13 de novembro

A 27ª Conferência Internacional de Segurança da Informação será realizada no Estádio Cívitas, organizada pelo ISMS Forum. Ela se concentra na gestão de sistemas de informação e regulamentações de segurança.

Link

Cibersegurança em tempo real: do alerta à ação

20 de novembro

A Ayesa está organizando este evento especializado das 10h às 14h em Madri, com foco na resposta imediata a ameaças e na transição da detecção para a ação corretiva.

Link

Recursos

➢ Check Point Infinity AI Security Services:

O Check Point Infinity foi reconhecido como a melhor plataforma de cibersegurança com tecnologia de IA, de acordo com o relatório de 2025 da Miercom. Sua arquitetura unificada oferece proteção abrangente para redes, nuvem, endpoints e dispositivos móveis, utilizando 50 mecanismos de IA que analisam big data de milhões de dispositivos conectados.

Seu sistema ThreatCloud integra inteligência avançada de ameaças com recursos Zero Trust e Secure Access Service Edge (SASE), oferecendo facilidade de uso e gerenciamento de segurança centralizado.

Link

➢ Plataforma de segurança Darktrace ActiveAI: detecção autônoma de ameaças

A Darktrace evoluiu sua plataforma para detectar ameaças aprendendo com o comportamento normal da rede, sem depender de assinaturas de ataque conhecidas. Sua capacidade de resposta autônoma Antigena pode conter ataques de maneira direcionada sem interromper as operações comerciais.
A plataforma usa análise comportamental para identificar anomalias de alto risco, incluindo ameaças sofisticadas baseadas em IA, estabelecendo modelos exclusivos para cada ambiente digital empresarial.

Link

➢ AccuKnox AI CoPilot: assistente de segurança para ambientes de nuvem

Uma nova ferramenta projetada especificamente para proteger aplicativos sem servidor, em contêineres e Kubernetes usando IA generativa. A AccuKnox usa a tecnologia eBPF para monitoramento detalhado do sistema, identificação de riscos, desenvolvimento de políticas de segurança e gerenciamento eficiente de crises.

Esta plataforma se destaca por seu foco na segurança nativa da nuvem sem comprometer as operações existentes, oferecendo detecção antecipada de ameaças e resposta automatizada.

Link

➢ Singularidade do SentinelOne: Proteção unificada com IA comportamental

O SentinelOne Singularity integra proteção, detecção e resposta unificadas para endpoints, cargas de trabalho em nuvem e identidades. Sua IA comportamental pode interromper *ransomware*, ameaças *zero-day* e ataques ativos usando modelos estáticos e comportamentais que operam em sistemas operacionais e ambientes de nuvem.

A plataforma inclui Purple AI para detecção de ameaças em linguagem natural, geração automática de resumos e aceleração de investigações, além de resposta automatizada baseada em políticas.

Link

NTT DATA Technology Foresight 2025

5 tendências que se tornarão realidade no ambiente empresarial.

Baixe o relatório: **es.nttdata.com/ntt-data-technology-foresight-2025**

Assine a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com