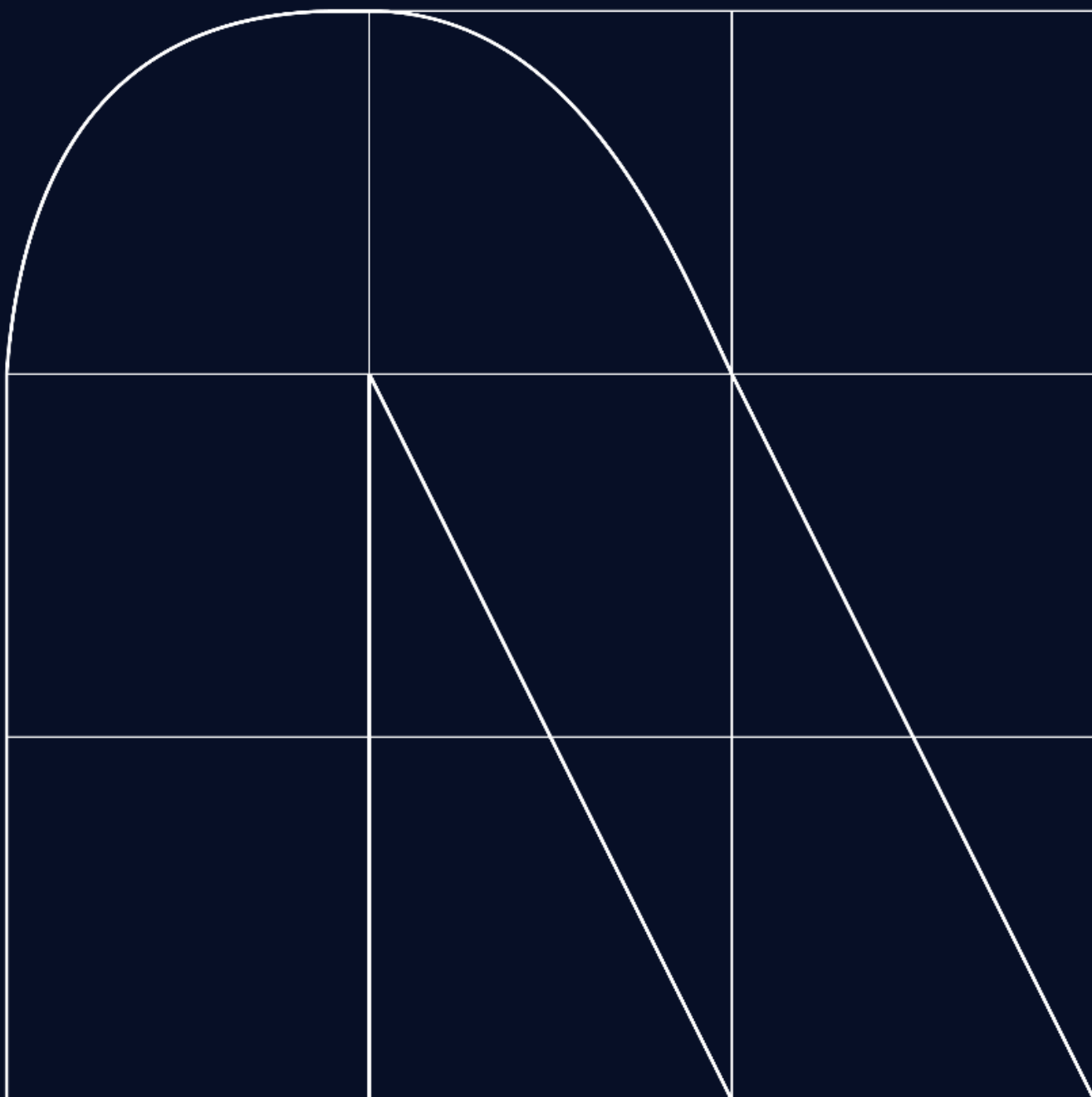
Número 86 | Janeiro de 2024

NTT DATA

# Radar

## A revista de cibersegurança



# 2024: Um novo início para o processo de transformação digital

Por Maria Pilar Torres Bruna

O ano de 2024 se inicia com a promessa de muita emoção no contexto da tecnologia. Quando pensávamos que as empresas tinham dado um grande passo em sua transformação digital (em decorrência da pandemia e da modernização que vem sendo imposta para continuarmos com o trabalho remoto), e que agora passaríamos por alguns anos de estabilização, novamente nos deparamos com a sensação de começo de jornada. Uma nova revolução está chegando, que será liderada pela adoção da inteligência artificial.

A começar pelas áreas de segurança, vimos como novos projetos de IA, embora na fase de prova de conceito, invadiram o campo dos negócios. A verdade é que mais de 70% das organizações, pelo menos na América Latina, reconhecem a IA como um motor de mudança na transformação que chega até nós. Há uma preocupação percebida do ponto de vista da segurança e da privacidade. Preocupação que já se tornou uma ocupação para diferentes governos que estão regulando o uso de inteligência artificial e entidades consolidadas como a NIST, a agência de proteção de dados pessoais da Espanha ou a rede ibero-americana de proteção de dados.

E nessa situação, só temos que fazer o que sempre fizemos: utilizar a cibersegurança como fundamento de alavancagem da transformação digital. E para a sua efetividade, os seguintes pontos devem estar bastante presentes no ano que se inicia:

- Devemos acompanhar a adoção de projetos de IA, garantindo que estejam em conformidade com uma estrutura de segurança e privacidade, que evite o viés e leve em consideração dados completos e fontes confiáveis. Não importa se o país em que estamos ainda não tem um regulamento em vigor. Vamos escolher uma estrutura robusta de boas práticas para nos preparar para futuras regulamentações e nos posicionar diante de nossos clientes como consumidores responsáveis da IA.
- Vamos adotar a IA para aumentar os níveis de segurança na empresa. Muitas tecnologias já trazem consigo o uso dela. Devemos maximizar esse uso e detectar pontos ainda não abrangidos para definir como tornar essa funcionalidade mais eficiente.
- A análise quantitativa de riscos pode ser uma grande aliada para demonstrar que investir em segurança, em projetos gerais e de IA, não apenas não é um custo, como também traz melhores resultados à médio prazo. Talvez seja hora de realizar a análise sobre os cenários de risco com maior impacto para a organização.
- Não vamos pensar no futuro. A cibersegurança não é mais um aspecto do CISO, mas uma questão de resiliência organizacional. Está nas mãos de todos.

Na NTT DATA, estamos convencidos de que um ano emocionante está chegando para aqueles como nós, que trabalham com cibersegurança. Estamos ansiosos para nos unir a você e continuar a crescer nesta área incrível. Feliz 2024! Desejamos a você um ano ciberseguro!

**Maria Pilar Torres Bruna**
Diretora de Cibersegurança

# Ataques cibernéticos ameaçam a segurança das infraestruturas médicas

Cibercrônica

Na estrutura global de saúde, uma ameaça digital silenciosa desencadeou uma vulnerabilidade sem precedentes na interseção entre tecnologia e saúde. No final de 2023, os ciberataques aumentaram drasticamente, figurando entre as mais afetadas as infraestruturas críticas de saúde, o que põe em risco a estabilidade de clínicas, hospitais, prestadores de serviços de saúde e laboratórios. Os defensores da saúde devem proteger um sistema frágil, cujo propósito é promover a saúde global.

Com o encerramento de novembro em Nova Jersey, o sistema de saúde local anunciou interrupções, marcando mais um episódio na cadeia de eventos que afetou a infraestrutura médica. A priorização das cirurgias, de acordo com a urgência, evidencia a grave vulnerabilidade de um sistema essencial, que serve de base não apenas para diagnósticos e tratamentos, mas também à sua própria existência.

Simultaneamente, em Tulsa, Oklahoma, o Hillcrest Medical Center tornou-se o epicentro de um ataque devastador de ransomware, que atrasou procedimentos vitais e expôs milhares de pacientes à incerteza sobre sua saúde. A realidade é que nossas vidas estão entrelaçadas com as complexidades digitais do serviço médico, de modo mais premente do que nunca.

> Esses ataques representam uma ameaça direta à vida e saúde de milhões, deixando os pacientes em espera e gerando custos econômicos devastadores

Continuou a se expandir para Nashville, Tennessee, quando a Ardent Health Services, responsável por 30 hospitais em seis estados, desconectou sua rede após um ataque cibernético também no final de novembro. Ambulâncias desviadas, procedimentos suspensos; a assistência médica, espinha dorsal da sociedade, se viu incapacitada diante dos ataques. A mesma ameaça angustiante estava presente na Colômbia em setembro de 2023, quando mais de 50 instituições estatais, incluindo a Superintendência Nacional de Saúde, relataram ataques cibernéticos sob a sinistra modalidade de ransomware, afetando seriamente a prestação de serviços aos cidadãos por várias instituições de saúde.

Esses eventos críticos revelam uma verdade arrepiante: o coração pulsante da saúde é vulnerável a ataques digitais que ameaçam não apenas a infraestrutura, mas diretamente a saúde e o bem-estar das comunidades. Nesse cenário, a cibersegurança não é apenas uma camada adicional, mas uma linha de defesa vital para proteger a integridade da saúde em todo o mundo. Ao mesmo tempo em que esses incidentes colocam em evidência as rachaduras no sistema, também exigem ações coletivas e imediatas para preservar a confiança e a eficácia dos serviços de saúde, garantindo que as ameaças cibernéticas não obliterem nossa capacidade de curar e cuidar.

Globalmente, centenas de ataques cibernéticos surgiram, desde as nações desenvolvidas até as menos favorecidas, em um jogo encabeçado pelos cibercriminosos, interessados tanto no lucro econômico, quanto na desestabilização e terrorismo social. A gravidade da situação exige ação imediata.

Esses ataques representam uma ameaça direta à vida e à saúde de milhões de pessoas, deixando os pacientes em espera e gerando custos econômicos devastadores. A colaboração internacional é um pilar crítico nesta batalha, por meio da qual as informações sobre ameaças devem ser compartilhadas de forma rápida e transparente para fortalecer as defesas coletivas.

A implementação de **estratégias de resposta rápida, tecnologias de inteligência artificial e aprendizado de máquina** torna-se essencial para detectar padrões de ataques antes que eles se materializem. Combater essa ameaça digital sombria requer não apenas inovação tecnológica, mas também mudança cultural e conscientização constante em todos os níveis do serviço de saúde. O investimento em inovações defensivas é imperativo para construir um escudo robusto contra aqueles que, partindo de cantos e recantos digitais obscuros, buscam sacrificar a saúde global. A vitória se dará não apenas pela proteção de dados, mas com a preservação da própria essência da nossa existência: a saúde e o bem-estar da humanidade.

No **início de 2024**, enfrentamos o desafio de transformar os obstáculos do passado em oportunidades de mudança e melhoria, em particular na defesa contra ameaças cibernéticas à saúde. A colaboração internacional e a inovação tecnológica são fundamentais para um futuro mais seguro, sustentadas por uma crescente consciência coletiva da importância da cibersegurança na medicina.
Este ano, estamos incumbidos da obrigação de traduzir as lições aprendidas na batalha cibernética em medidas mais eficazes, no sentido de construir um escudo mais forte contra as ameaças digitais. Maio de 2024 será um período de transformação positiva, em que a união global, a tecnologia avançada e a conscientização constante nos levarão a uma segurança cibernética fortalecida e, em última instância, a um serviço de saúde mais seguro e confiável para todos.

Mas não só o setor de saúde está sendo afetado pelos implacáveis cibercriminosos, já que neste momento um malware antigo retornou com mais força, e surgiram novas formas de violar os setores público e empresarial, bem como todos os usuários da internet. Por esse motivo, vale mencionar um RAT que ressurgiu fortemente: **o NetSupport RAT**. Os Trojans de Acesso Remoto (RATs) são mestres em orquestrar o caos, fornecendo ao invasor controle absoluto sobre a máquina infectada. Ao se infiltrar em um sistema, esse malware estabelece uma ponte virtual, permitindo que o intruso dirija o dispositivo remotamente, tal e qual ferramentas como o Protocolo de Área de Trabalho Remota (RDP) ou o TeamViewer.

O NetSupport RAT, outrora uma ferramenta legítima de administração remota conhecida como NetSupport Manager, renasceu como uma ameaça latente nas mãos de agentes maliciosos. Os especialistas em segurança observam com preocupação o aumento dramático das infecções, que têm entre suas vítimas setores críticos como a educação, o governo e os serviços empresariais. A disseminação do NetSupport RAT é produzida por meio de vários truques, desde atualizações fraudulentas até downloads clandestinos. Este Trojan se destaca por sua versatilidade em afetar desde ciberneófitos até adversários experientes, tornando-se uma ameaça de escopo amplo e sutil.

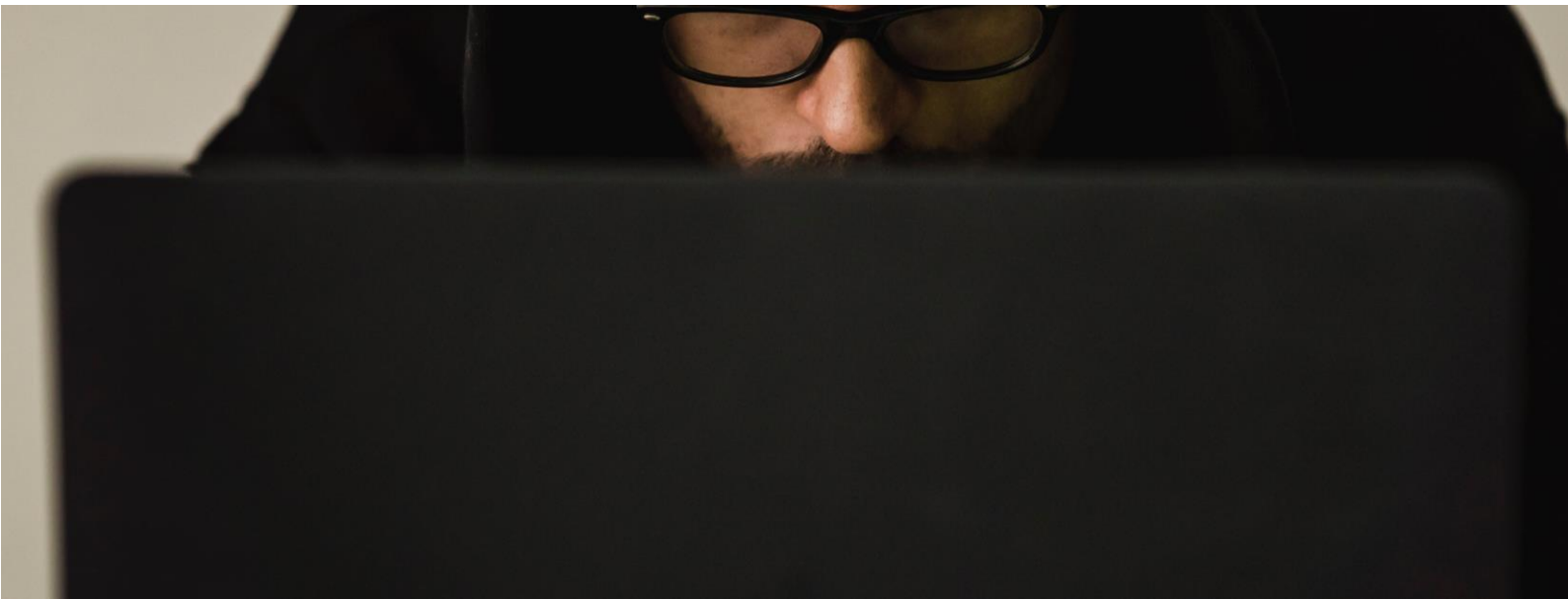
O modus operandi do NetSupport RAT envolve enganar as vítimas para que baixem atualizações falsas do navegador de plataformas comprometidas. Essa tática de infecção adaptativa e astuta deixa uma marca sutil, mas inconfundível, na tela em constante mudança da cibersegurança. Diante de tal ressurgimento sorrateiro, a cibersegurança deve adotar uma abordagem vigilante e estratégica. A conscientização do usuário é um escudo essencial, partindo de sua educação sobre táticas de phishing e cautela ao baixar atualizações. Implementar soluções avançadas de segurança e manter a infraestrutura de tecnologia atualizada, tornam-se barreiras cruciais para conter o ataque do NetSupport RAT.

**O NetSupport RAT pode desencadear consequências devastadoras** quando consegue se infiltrar em um sistema. Os invasores, armados com esse malware, podem executar várias ações maliciosas, como roubar dados confidenciais, controlar remotamente o sistema afetado e até interromper serviços essenciais. Esse conjunto de capacidades ameaça não apenas a confidencialidade das informações, mas também causa perdas financeiras e prejudica a reputação das vítimas. A presença do NetSupport RAT tem sido detectada em diversos setores, desde a educação até os serviços empresariais. Escolas, universidades, entidades governamentais e empresas têm sido alvo trojan de acesso remoto, ressaltando a amplitude de sua ameaça. O NetSupport RAT emprega uma variedade de métodos para se espalhar, incluindo o phishing, a injeção de código e o download manual de malwares. A diversidade de estratégias faz com que a detecção e a prevenção sejam desafios constantes neste jogo estratégico no ciberespaço.

Nesse cenário, a **defesa contra o renascimento do NetSupport RAT** requer medidas preventivas robustas. A conscientização do usuário, uma política rígida de atualizações, o investimento em soluções avançadas de segurança, a atualização constante dos sistemas e a implementação de sistemas de monitoramento contínuo são recomendações essenciais para mitigar riscos e proteger o ambiente cibernético. A colaboração entre a comunidade da cibersegurança é uma força compartilhada, uma união de forças para compreender e neutralizar as ameaças emergentes. Neste embate dinâmico entre atacantes e defensores, cada medida de mitigação é um passo crucial para preservar a integridade digital no mundo interconectado.

**Martín Bedoya**
Analista Líder de Cibersegurança

**Orlando Ospina**
Analista de Cibersegurança



# BEM-VINDO(A) AO ANO DE 2024. AS TENDÊNCIAS DE cibersegurança MUDARÃO?

TENDÊNCIAS

No final do ano, costumamos avaliar o panorama da cibersegurança nas empresas. Neste fim de ano, observamos que, apesar de haver processos contínuos de avaliação de risco, elas não conseguem reduzir a sua exposição a ameaças, pois ainda persistem em abordagens irrealistas, isoladas e focadas em ferramentas.

A Forbes indicou que, até o final de 2024, o custo dos ataques cibernéticos para a economia global irá superar os US$ 10,5 trilhões. Esses números demonstram uma necessidade crescente na questão da cibersegurança e sua prioridade estratégica no nível individual e organizacional. Temos nos preparado para enfrentar novas tendências e tecnologias em nossas organizações, falar sobre a Internet das Coisas (IoT), Big Data, 5G e, mais recentemente, a Inteligência Artificial (IA), nos leva a pensar não apenas em novas oportunidades de negócios, mas também nas novas formas como os cibercriminosos podem nos atacar. Mas nos deparamos com um cenário completamente fora da realidade quando observamos que essas "novas formas" permanecem sendo as mesmas que "combatemos" ano após ano:

Por exemplo, organizações como a CISA (Cybersecurity & Infrastructure Security Agency) e a ENISA (European Union Agency for Cybersecurity) concordam que, considerando o impacto e a frequência com que as várias ameaças podem ser realizadas ou identificadas, podemos considerá-las nos seguintes grupos:

- Ransomware
- Malware
- Engenharia social
- Ameaças de dados
- Ameaças à disponibilidade
- Manipulação das informações
- Ataques na cadeia de suprimentos (supply chain)

À medida que as organizações lutam para acompanhar um cenário de ameaças em constante evolução, os líderes de cibersegurança tendem a recorrer a abordagens reativas, que se limitam à busca constante por ameaças, visando minimizar possíveis incidentes. Isso vai de encontro a uma estratégia de iniciar e amadurecer programas com uma nova abordagem voltada à compreensão da superfície de ataque, a qual estão expostas. Acreditamos que essa seria a abordagem que lhes permitiria priorizar melhor seus esforços e mensurar o progresso ao longo do tempo.

**As recomendações nesta situação são:**

• Garantir que os resultados do gerenciamento de exposição contribuam para várias partes das organizações de segurança e TI, concebendo um programa para gerenciar um conjunto mais amplo de exposições.

• Considerar cenários de exposição a ameaças usando áreas emergentes e associadas ao gerenciamento da superfície de ataque, bem como uma postura de segurança.

• Integrar a gestão contínua de exposição a ameaças e pôr em prática um processo de cinco etapas a cada ciclo (escopo, descoberta, priorização, validação e mobilização), de forma associada ao fluxo de gestão de incidentes.

# Criptografia da camada de aplicação como estratégia para fortalecer a postura de segurança

A criptografia se estabeleceu como uma ferramenta fundamental para salvaguardar a confidencialidade das informações. Por meio de mecanismos matemáticos, é possível transformar um conjunto de dados a fim de evitar que agentes não autorizados o decifrem. Esse processo é fundamental quando se trata de proteger o tráfego dos sistemas que são implantados pela internet.

O protocolo Transport Layer Security (TLS) desempenha um papel crucial na segurança das informações transmitidas nas comunicações entre um servidor e um cliente. É responsável por adicionar o bloqueio ao navegador, no que é conhecido como HTTPS. Operando na camada de transporte, este protocolo é responsável por criptografar todo o canal de comunicação utilizando suites de criptografia.

Atividades como troca de chaves, autenticação mútua, criptografia e revisão de integridade por meio de hashes são processos que são realizados graças ao TLS, que garante confidencialidade, integridade e não repúdio, verificando se as partes envolvidas são quem dizem ser e não podem negar a autenticidade das informações trocadas. Esse processo abrangente de criptografia é um componente essencial na proteção contra ameaças e permite a troca segura de dados.

Embora o protocolo TLS garanta um canal de comunicação criptografado pela internet, é importante observar que a criptografia se aplica exclusivamente ao canal. Isso significa que, na prática, existe a possibilidade de capturar e manipular informações abusando da confiança do protocolo TLS. Portanto, como uma medida de defesa em profundidade, a criptografia da camada de aplicativos permite adicionar controle adicional para proteger os dados de solicitações que trafegam pela Internet.

Os proxies https são ferramentas que permitem a execução de ataques conhecidos como "*Man In The Mide*", pois possuem a capacidade de interferir no protocolo TLS abusando de sua excessiva confiança no navegador. Esses proxies permitem que um invasor observe e altere os parâmetros que são enviados de um cliente para o servidor em um aplicativo web ou móvel, mesmo quando as informações são protegidas por TLS. Como essas ferramentas são amplamente conhecidas pelos adversários, é necessário considerar estratégias de segurança adicionais para proteger o tráfego.

Capturar o tráfego de rede de um aplicativo Web ou móvel introduz uma série de ameaças que devem ser levadas em conta a partir do conceito da solução. Injeções de código, ataques de força bruta, enumeração de usuários ou sequestros de sessão são ataques comumente conhecidos que podem ser realizados graças à possibilidade de inspecionar o tráfego de aplicativos.

Para combater essas ameaças potenciais, é possível implementar a criptografia na camada de aplicação. Este controle se concentra em proteger a confidencialidade dos parâmetros que são enviados em solicitações e respostas do servidor. Nesse sentido, as fábricas de software devem implementar esse controle diretamente no aplicativo, ou seja, no código-fonte do backend e do frontend.

Os programadores podem usar dois conceitos fundamentais de criptografia: criptografia simétrica e assimétrica. Um algoritmo de criptografia simétrica envolve o uso de uma única chave para o processo de criptografia e descriptografia. Essa abordagem, embora eficiente, impõe o desafio de compartilhar com segurança a chave entre as partes da comunicação. Por outro lado, as cifras assimétricas usam um par de chaves: uma pública e uma privada. A chave pública é compartilhada abertamente, enquanto a chave privada é mantida em segredo. As informações criptografadas com chave pública só podem ser efetivamente descriptografadas com a chave privada correspondente.

A escolha do tipo de algoritmo de criptografia a ser utilizado deve ser definida a partir da fase de projeto do aplicativo. Por um lado, a criptografia simétrica, por ser mais leve, permite que os dados sejam criptografados mais rapidamente. No entanto, ela traz o risco de que a chave compartilhada seja capturada e o adversário consiga descriptografar a comunicação.

Para resolver esse problema, os programadores podem implementar mecanismos de ofuscação por obscuridade para ocultar a chave. Por outro lado, a criptografia assimétrica proporciona maior segurança, uma vez que a chave de descriptografia não é compartilhada. Apesar disso, os algoritmos de criptografia assimétrica exigem maior capacidade computacional devido à complexidade algorítmica, o que pode impactar seriamente o desempenho e a experiência do usuário do aplicativo. Portanto, a implementação da criptografia na camada de aplicação deve ser um controle que deve ser implementado com base em uma análise e conhecimento aprofundado das necessidades do negócio.

É importante considerar que a não aplicação de criptografia na camada de aplicação introduz várias ameaças aos aplicativos. No entanto, a fundação OWASP, que é uma comunidade aberta relacionada à segurança de aplicativos, não se aprofunda nesse controle em suas diferentes estruturas metodológicas, isso pode ser devido ao impacto no desempenho do aplicativo e no custo de implementação para a fábrica de software.

Historicamente, a segurança e o desempenho seguiram em direções opostas. No entanto, nos últimos anos, as capacidades de computação experimentaram um aumento significativo no poder e uma redução considerável nos custos graças à nuvem, tornando a implementação da criptografia na camada de aplicação mais viável.

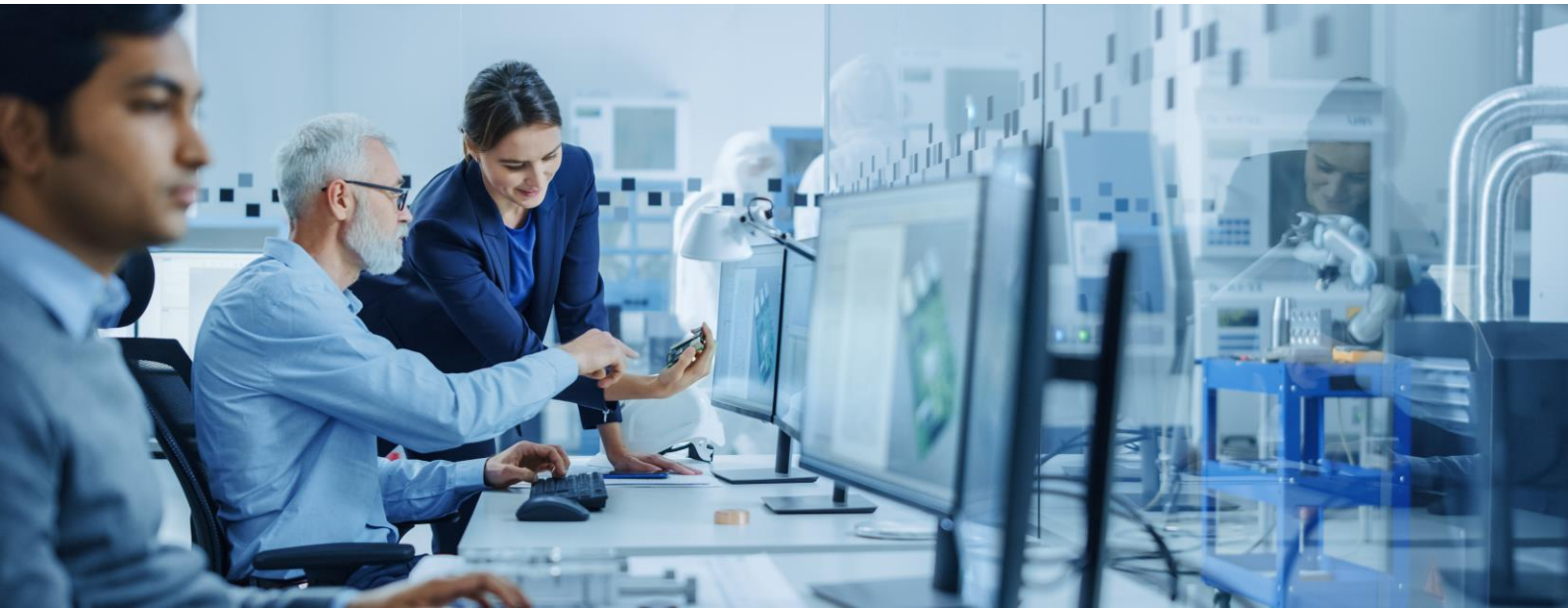
Por outro lado, encontrar programadores que implementem criptografia pode ser um desafio para as fábricas de software; a necessidade de programadores mais experientes aumenta o custo por hora de desenvolvimento, custos estes que têm representado uma barreira significativa para a adoção generalizada da criptografia da camada de aplicativos. No entanto, atualmente há uma mudança nesse cenário graças ao aumento das bibliotecas *OpenSource* e da documentação relacionada sobre como criptografar em linguagens de programação para a web.

Apesar desse progresso, a OWASP ainda não incluiu a interceptação de tráfego como critério de vulnerabilidade para aplicativos Web; até o momento, só o fez para aplicativos móveis, tendo sido um controle posteriormente desprezado. As prioridades e abordagens de segurança mudam ao longo do tempo à medida que as tecnologias e as ameaças cibernéticas evoluem. É crucial que as fábricas de software acompanhem as práticas de segurança atualizadas e antecipem as mudanças no ambiente tecnológico que introduzem novas ameaças. É provável que a OWASP incorpore esse controle em suas próximas atualizações.

Em suma, o protocolo TLS, embora valioso para proteger o canal de comunicações, não é suficiente para garantir a proteção das informações contra interceptação. Portanto, a implementação da criptografia da camada de aplicação é uma estratégia de segurança que pode ser usada pelas fábricas de software para fortalecer sua postura de segurança e aumentar o nível de maturidade na segurança de aplicativos. Todos os dias, a implementação desse controle é mais econômica e seus benefícios são facilmente mensuráveis, pois a motivação de um adversário para comprometer um aplicativo pode ser diminuída quando ele não deve apenas evitar o TLS, mas uma camada adicional de criptografia.

**Martín Bedoya**
Analista Líder de Cibersegurança

**José Cianci**
Analista de Cibersegurança



# Neobancos e tendências em cibersegurança: desafios e oportunidades

Nos últimos anos, o setor financeiro passou por uma grande transformação digital que levou, entre outros aspectos, à chegada dos neobancos, que são entidades financeiras que oferecem seus serviços sob um esquema totalmente digital, sem as tradicionais agências físicas, apostando em uma diferenciação na agilidade e praticidade para o registro dos usuários, bem como na aquisição e uso de seus produtos.

À medida que os neobancos se posicionam no mercado e agregam cada vez mais usuários, a cibersegurança surge como um elemento-chave nesse novo cenário financeiro. Neste artigo, exploraremos alguns dos principais desafios e oportunidades com os quais atualmente se deparam os neobancos, no campo da cibersegurança:

**Desafios que os neobancos devem levar em conta**

**Autenticação reforçada:** a autenticação segura é essencial em um ambiente financeiro totalmente digital, implementar medidas como a autenticação multifator e as tecnologias biométricas se torna essencial para garantir os processos de validação de identidade do usuário, bem como a execução segura das operações.

**Aumento e evolução das ameaças cibernéticas**: sua proposta de valor 100% digital os torna um alvo muito atraente para ataques cibernéticos como phishing, ransomware, negação de serviço, fraudes on-line, entre outros; o que poderia comprometer seriamente a segurança das informações financeiras e pessoais dos usuários.

**Armazenamento em nuvem**: a grande maioria dos neobancos armazena dados em nuvem para facilitar o acesso e a agilidade em seus serviços, o que exige a implementação de medidas de segurança mais avançadas para protegê-los.

**Privacidade de dados pessoais:** a coleta e o processamento de dados são fundamentais para o funcionamento dos neobancos; garantir a privacidade e a segurança dessas informações pessoais é fundamental para desenvolver e manter a confiança de seus clientes.

**Conformidade regulatória:** à medida que os neobancos se expandem, enfrentam desafios em termos de conformidade regulatória, pois as regulamentações de segurança cibernética e privacidade também estão evoluindo e se tornando cada vez mais exigentes com esse tipo de propostas inovadoras no mercado financeiro; nesse sentido, os neobancos devem se adaptar e garantir o cumprimento dessas regulamentações, a fim de evitar possíveis multas ou sanções.

**Educação do usuário:** a conscientização e a educação do usuário são componentes-chave na defesa contra ameaças cibernéticas. Os neobancos devem fornecer informações claras sobre as melhores práticas de segurança, identificação de ameaças potenciais e como os usuários podem se proteger.

**Oportunidades em meio a desafios**

Assim como existem vários desafios na cibersegurança, os neobancos também têm a oportunidade de se diferenciar e desenvolver a confiança do usuário por meio de medidas proativas.

Eles contam com uma ampla gama de opções para investir em ferramentas de segurança e tecnologias emergentes, como a inteligência artificial, aprendizado de máquina, inteligência contra ameaças, entre outras, para antecipar riscos e fortalecer suas defesas.

Além disso, podem incrementar e/ou melhorar suas capacidades por meio de provedores especializados, que ofereçam conhecimento especializado e soluções avançadas para os diferentes desafios que devem enfrentar em termos de cibersegurança.

Em conclusão, à medida que os neobancos abrem novas possibilidades no cenário financeiro, a cibersegurança se torna um pilar fundamental de seu sucesso e sustentabilidade. A adoção de tecnologias emergentes e o suporte de fornecedores experientes em cibersegurança permitirão que prosperem em um ambiente cada vez mais dinâmico e ameaçador. A chave está na capacidade de manter um equilíbrio entre inovação e segurança para fornecer serviços financeiros digitais confiáveis.

**Milagros Silvia**
Consultora Especializada em Cibersegurança

# Gestão de Continuidade de Negócios: TI e TO

A Gestão de Continuidade de Negócios (GCN) é o conjunto de atividades, processos, ferramentas, pessoas e controles previamente definidos, estruturados, documentados e testados, que visam garantir a continuidade mínima, previamente acordada, dos serviços e/ou áreas que dão suporte ao negócio, quando um ou mais recursos relevantes para a organização não estiverem disponíveis. A GCN permite que a organização tenha um menor impacto, uma certa previsibilidade e uma continuidade adequada das suas atividades.

A Governança Corporativa tem princípios. Um deles exige sustentabilidade. Como tal, a existência da GCN é da responsabilidade do Conselho de Administração e/ou da Direção.
1. Transparência: Relatar e disponibilizar as informações corretamente.
2. Equidade: Tratamento justo e não discriminatório.
3. Prestação de contas: Responsabilidade.
4. Continuidade corporativa: Sustentabilidade da organização.

**Tipos de recursos**

Para uma melhor estruturação, implementação e manutenção da GCN, é importante identificar que tipos de recursos existem e quais devem ser considerados.

**Recursos de Tecnologia da Informação (TI):** recursos em que informações ou dados são os principais elementos a serem considerados em suas diversas formas e apresentações. Esse conjunto de recursos é o mais conhecido e utilizado nas organizações. É o mais avançado em termos de processamento e comunicação. Possui alta maturidade de segurança.

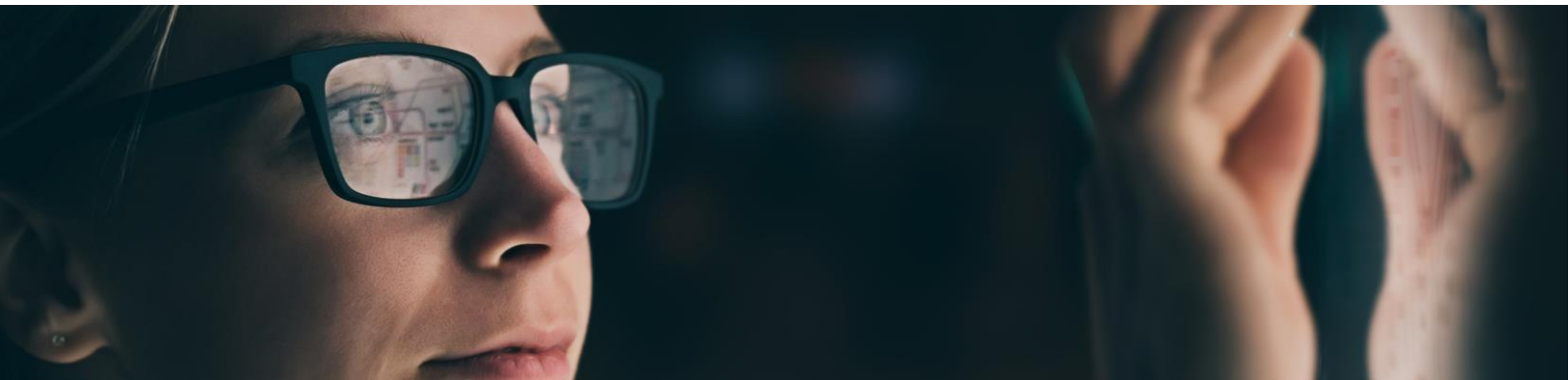
**Recursos de Tecnologia Operacional (TO):** quando o recurso a ser considerado não for, em sua essência, de natureza informacional ou de dados. Este grupo inclui equipamentos com algum processamento para as áreas industrial, sanitária e agroindustrial. São recursos da Internet das Coisas (IoT). Existem muitos tipos de equipamentos.

Considerando os controles de confidencialidade, integridade, disponibilidade, legalidade, não repúdio e confiabilidade, todos eles são importantes para o funcionamento das organizações. No entanto, há um direcionador de segurança para cada tipo de tecnologia. Para as tecnologias da informação, a prioridade é a confidencialidade. Para tecnologias operacionais, a prioridade é a disponibilidade. Os outros controles vêm em sequência.

A Segurança para Tecnologia da Informação está mais madura e tem equipamentos, aplicações, legislação e padrões definidos. A Segurança para Tecnologia Operacional é menos madura, devido à sua necessidade de segurança. Até recentemente, a TO lidava com o ambiente de máquinas industriais, com operação muito limitada a equipamentos ou grupos de equipamentos que costuma ter uma fábrica. Com o desenvolvimento da Internet das Coisas (IoT), o campo da Tecnologia Operacional tornou-se mais sofisticado e foi além do ambiente industrial. O agronegócio está usando sensores de solo para indicar umidade e outros fatores em grandes campos, bem como para monitorar suas máquinas. O setor de saúde está usando equipamentos de exame, operações remotas com robôs ou máquinas intracorpóreas, como marca-passos e chips que coletam informações do corpo. As cidades inteligentes estão crescendo e gerando instalações e cuidando da privacidade dos cidadãos.

Mas, seja Tecnologia da Informação ou Tecnologia Operacional, deve haver Planos de Continuidade de Negócios. Os controles em nível macro são os mesmos. No entanto, em cada um deles haverá uma aplicação específica para informações ou “coisas” inteligentes.

As etapas descritas a seguir são indicativas e devem ser sempre utilizadas levando em consideração as características do ambiente a ser protegido. Elas são subdivididas da seguinte forma (próxima página)



**Identificação de ameaças:**
Todas as possíveis ameaças devem ser identificadas. No entanto, as ameaças que serão consideradas para o plano devem ser definidas.

**Escopo e cenário:**
O escopo corresponde à gama de recursos e ambientes que serão considerados. O cenário corresponde ao tempo e às condições específicas da possível situação de indisponibilidade.

**Priorização de recursos:**
É a definição da ordem de prioridade e tempo para a recuperação dos recursos. O Tempo Máximo de Recuperação (RTO) e o Ponto de Recuperação (RPO) são identificados levando em consideração a perda de dados. Essa priorização pode ser identificada por um processo de Análise de Impacto nos Negócios (BIA), um requisito contratual, um requisito legal ou uma definição do Conselho de Administração.

**Seleção de estratégia:**
Trata-se de definir a solução alternativa para o recurso ou ambiente. As prioridades e o custo de implementação da solução alternativa serão considerados.

**Estruturação e elaboração do plano:**
Trata-se de projetar o equipamento, fluxo, atividades, responsabilidades e documentação.

**Planejamento e condução de testes:**
É o planejamento, elaboração, estruturação, autorização, execução e avaliação dos testes.

**Manutenção do plano:**
Trata-se do planejamento e das regras de atualização periódica e atualização específica.

**Plano de crise e plano de comunicação:**
Do ponto de vista da GCN, o Plano de Crise e o Plano de Comunicação existem para respaldar e possibilitar o desempenho holístico de todas as áreas da organização. Decerto, eles podem ter uma vida independente, mas na prática se complementam e permitem a eficácia dos outros planos.

**Plano de crise:**
Conjunto de ações e controles a serem planejados pela organização quando ocorrer um evento inesperado que possa ter um impacto negativo na organização.

**Plano de comunicação**:
Este plano garante a existência de comunicação interna dentro da organização e também (principalmente) a comunicação da organização com o ambiente externo, como a imprensa, clientes, acionistas, órgãos de fiscalização ou similares.

**A Gestão de Continuidade de Negócios:**
Deve ser concebida e construída especificamente para cada organização e cada situação organizacional. Não existe um "plano pré-fabricado". Os profissionais envolvidos na gestão da continuidade dos negócios devem ter conhecimento e experiência em planos e situações de contingência.

**Edison Goncalves**
Evangelista de Cibersegurança

# Vulnerabilidades

## Várias vulnerabilidades em dispositivos Dell

Data: 4 de dezembro de 2023
CVE: CVE-2023-44304 e mais 1

**CVSS: 9.8**

**CRÍTICA**

### Descrição

A Dell relatou várias vulnerabilidades em seu produto "Dell DM5500", em todas as versões anteriores à 5.14.0.0. Dentre elas, destacam-se duas de vulnerabilidade crítica.

Uma dessas vulnerabilidades, a CVE-2023-44302, permite que um invasor obtenha acesso ao dispositivo sem se autenticar previamente a ele, com a possibilidade de executar código remoto e obter o controle do computador afetado.

Além disso, a outra vulnerabilidade crítica descoberta neste dispositivo recebe o identificador CVE-2023-44304. Essa vulnerabilidade está associada à elevação de privilégios, permitindo que um invasor com baixos privilégios de segurança ignore as restrições que ele contém por sua função, permitindo o acesso à raiz do dispositivo e visualização de seu conteúdo.

Além disso, outras vulnerabilidades de menor gravidade também foram descobertas, também associadas ao escalonamento de privilégios.

### Produtos impactados

Esta vulnerabilidade afeta as seguintes versões:

- Todas as versões anteriores a 5.14.0.0.

### Solução

A Dell emitiu um aviso (DSA 2023-425) informando que a correção principal para essa vulnerabilidade é atualizar para a versão mais recente do dispositivo.

### Links

- www.dell.com
- nvd.nist.gov
- www.cvedetails.com

## Vulnerabilidade crítica no software Apache Struts

Data: 7 de dezembro de 2023
CVE: CVE-2023-50164

**CVSS: 9.8**

**CRÍTICA**

### Descrição

Em 7 de dezembro de 2023, uma vulnerabilidade foi publicada no software Apache Struts, uma ferramenta de suporte para o desenvolvimento de aplicativos Web com uso de Java.

A vulnerabilidade crítica, uma vez explorada, pode permitir que um invasor execute código remoto no dispositivo afetado.

Para executar o código remoto, um invasor deve aproveitar uma configuração incorreta no servidor, realizando um ataque "Path Transversal". A partir deste ponto, existe a possibilidade de fazer upload de um arquivo para o próprio servidor web que permita a execução remota de código nele.

Esta vulnerabilidade foi identificada como CVE-2023-50164, e o Apache aconselhou seus usuários a atualizar para as novas versões a fim de corrigir essas falhas de segurança o mais rápido possível.

### Produtos impactados

Os diferentes produtos afetados por esta vulnerabilidade são os seguintes:

- Versões anteriores a 2.5.33.
- Versões anteriores a 6.3.0.2.

### Solução

A solução proposta pelo fabricante consiste na atualização para as versões citadas acima:

- Versão 2.5.33.
- Versão 6.3.0.2.

### Links

- www.incibe.es
- lists.apache.org

# Patches

CRÍTICA

## Vários patches de segurança para dispositivos Android

Data: 4 de dezembro de 2023
CVE: CVE-2023-40077 e mais 4

### Descrição
O Android lançou novos patches de segurança que corrigem uma grande quantidade de vulnerabilidades em todos os seus dispositivos, alguns dos quais são classificadas como críticas.

As quatro vulnerabilidades críticas são detalhadas abaixo:
- CVE-2023-40077: vulnerabilidade de escalonamento de privilégios.
- CVE-2023-40076: que permite o acesso a credenciais de outros usuários.
- CVE-2023-40088: vulnerabilidade que permite corrupção de memória.
- CVE-2023-45866: vulnerabilidade que permite injeção de mensagem HID.
- CVE-2022-40507: vulnerabilidade que permite corrupção de memória.

As vulnerabilidades afetam tanto o sistema operacional, quanto os componentes do sistema, a estrutura, a MediaTek e a Qualcomm.

### Produtos impactados
Os seguintes produtos foram afetados por essas vulnerabilidades:
- Android (versão 14)
- Android (versão 13)
- Android (versão 12L)
- Android (versão 12)
- Android (versão 11)

### Solução
A solução consiste em atualizar os patches de segurança publicados no boletim de dezembro (dependendo da versão do sistema operacional instalado em cada caso).

### Links
- source.android.com
- www.csa.gov.sg
- www.incibe.es

CRÍTICA

## Novos patches de segurança para produtos Microsoft

Data: 12 de dezembro de 2023
CVE: CVE-2023-35618 e mais 1

### Descrição
Em 12 de dezembro, a Microsoft lançou uma série de atualizações para corrigir várias vulnerabilidades de segurança em seus sistemas operacionais Windows e outros *softwares*. No total, foram publicadas 36 vulnerabilidades, das quais 2 são críticas, 23 importantes e 11 de gravidade média.

Abaixo estão as vulnerabilidades categorizadas como críticas:
- CVE-2023-35618: vulnerabilidade que afeta o Microsoft Edge. Uma vez que este aplicativo é violado, é possível obter os privilégios necessários para executar o código na máquina violada.
- CVE-2023-36019: esta vulnerabilidade afeta os serviços Microsoft Power Platform e Azure Logic Apps. Ela se concentra em um ataque de "*spoofing*" que tem início ao clicar em um link fornecido pelo invasor, redirecionando a vítima para outro link ou arquivo malicioso.

O restante das vulnerabilidades pertence a vários tipos: negação de serviço, escalonamento de privilégios, divulgação de informações, execução remota de código e phishing.

### Produtos impactados
Essas vulnerabilidades abrangem um grande número de produtos da Microsoft. Esses produtos podem ser encontrados em: msrc.microsoft.com

### Solução
Aplique o patch de segurança correspondente nos produtos afetados.

### Links
- msrc.microsoft.com
- thehackernews.com

# Eventos

### SANS Cloud Defender 2024 (ao vivo on-line) (8 a 13 de janeiro)

O SANS Cloud Defender 2024 acontecerá on-line de 8 a 13 de janeiro. Este curso oferece treinamento imersivo concebido para profissionais de segurança e/ou TI interessados em aprender como construir, implantar e gerenciar infraestrutura, plataforma e aplicativos seguros na nuvem.

**Link**

### CSA AI Summit (17 - 18 de janeiro)

O CSA AI Summit é um evento de grande porte que busca reunir especialistas do setor para fornecer orientações sobre questões críticas da Inteligência Artificial (IA) e seu impacto na cibersegurança. Ao longo de dois dias, ele oferece insights importantes sobre como a IA generativa pode beneficiar a cibersegurança, como ela está sendo usada por invasores cibernéticos e diretrizes que devem ser consideradas para uso responsável.

**Link**

### SANS Cyber Threat Intelligence Summit & Training 2024 (29 de janeiro a 5 de fevereiro de 2024)

O SANS Cyber Threat Intelligence Summit & Training é um evento que acontece em Washington, Estados Unidos, de 29 de janeiro a 5 de fevereiro. Este evento, que também pode ser acessado on-line, visa permitir que as partes interessadas do setor obtenham novas perspectivas e aprendam com estudos de caso que desafiam as suposições da inteligência de ameaças cibernéticas, levando a uma mudança em seu entendimento.

**Link**

# Recursos

**FAQ do Certificado de Competência Zero Trust (CCZT):**
O Certificado de Competência Zero Trust (CCZT) é um recurso líder do setor que fornece aos profissionais de tecnologia o conhecimento essencial para entender e aplicar os princípios de Zero Trust. Mais informações sobre os benefícios do CCZT e como acessá-lo podem ser encontradas no documento de perguntas frequentes preparado pela Cloud Security Alliance (CSA).

Link

**Mitigação de riscos de segurança em aplicativos baseados em LLM de Geração de Recuperação Aumentada (RAG)**

A Geração de Recuperação Aumentada é uma técnica eficaz usada por engenheiros de IA para desenvolver aplicativos baseados em grandes modelos de linguagem (LLMs). No entanto, foi identificado que a falta de controles de segurança em aplicativos LLM baseados em RAG pode representar riscos se não for tratada adequadamente. Por conta disso, o artigo elaborado pela Cloud Security Alliance, tem como objetivos: (i) analisar a arquitetura RAG, (ii) identificar potenciais riscos de segurança em cada etapa; e, (iii) fornecer recomendações técnicas para mitigar esses riscos, servindo assim como um guia prático para os desenvolvedores.

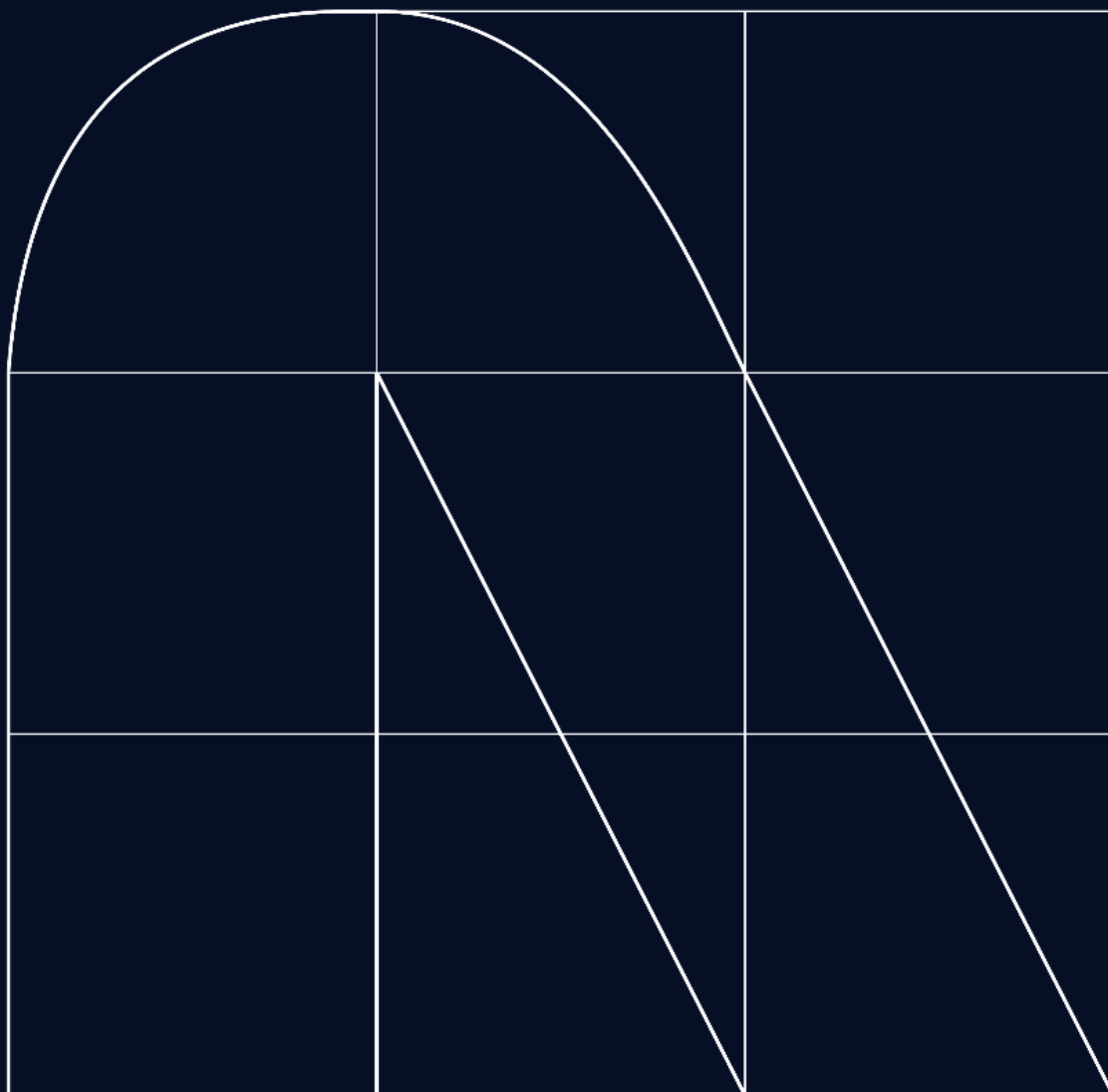
Link

**GPT-4 Turbo**

A OpenAI anuncia o lançamento do GPT-4 Turbo, uma nova geração do modelo de linguagem grande (LLM), que promete superar as deficiências dos anteriores, GPT-3.5 e GPT-4, além de ser mais rápido e barato. Esta nova versão atinge um comprimento de contexto de 128.000 tokens, ou seja, a quantidade de texto que suporta e entende quando o chatbot recebe uma pergunta. Além disso, ele pode aceitar imagens como entradas na API Chat Completions, permitindo casos de uso como geração de legendas, análise detalhada de imagens do mundo real e leitura de documentos com figuras.

Link





**Desenvolvida pela equipe de cibersegurança da NTT DATA**

es.nttdata.com