Número 115 | Junho de 2026

NTT DATA

Radar

A revista de cibersegurança

Quando as máquinas aprendem a atacar infraestruturas reais

Por Luís Guillen

A convergência entre a inteligência artificial e os sistemas de tecnologia operacional criou um novo campo de batalha híbrido, no qual não basta proteger dados. Agora, também está em jogo a continuidade do mundo físico. Não é a mesma coisa falar do roubo de dados de um cartão de crédito e de uma interrupção no fornecimento de energia elétrica de uma população, da paralisação de uma planta de tratamento de água ou do desencadeamento de uma falha em cadeia em uma refinaria.

No primeiro caso, falamos de um incidente grave, enquanto, no segundo, falamos de um cenário potencialmente catastrófico, com impacto direto sobre a segurança das pessoas. Durante anos, a cibersegurança separou o mundo digital do mundo físico, mas hoje essa fronteira praticamente desapareceu, e a inteligência artificial está derrubando os últimos limites.

Os sistemas de tecnologia operacional funcionam como o sistema nervoso da indústria. Falamos de controladores lógicos programáveis (PLC), sistemas SCADA, sensores industriais e toda a infraestrutura digital que governa processos físicos, incluindo componentes que controlam edifícios inteligentes e equipamentos médicos, ou seja, desde a abertura de uma válvula ou a gestão do tráfego ferroviário até o funcionamento de elevadores, circuitos de televisão, sistemas de imagem médica e respiradores hospitalares conectados. Durante décadas, esses ambientes permaneceram relativamente isolados das redes corporativas.

Sua segurança se apoiava, em boa parte, no famoso "air gap", a separação física que protegia esses ambientes contra ameaças externas. Esse modelo ficou no passado. A pressão por eficiência operacional, monitoramento remoto e integração com sistemas empresariais foi reduzindo essa distância. Hoje, a maioria dos ambientes OT/IoT está conectada, direta ou indiretamente, a redes expostas ao exterior. E isso os transforma em alvos.

A IA como um multiplicador de ameaças

A exposição desses ambientes já era preocupante. Com a entrada da inteligência artificial no ecossistema dos ciberataques, a ameaça passa a uma dimensão completamente nova. Não estamos falando de ficção científica. Estamos falando de ferramentas que já existem, evoluem a cada mês e estão ao alcance de agentes com recursos que, até pouco tempo atrás, eram exclusivos dos Estados mais avançados.

A IA permite que agentes maliciosos automatizem o reconhecimento de infraestruturas, identifiquem vulnerabilidades em protocolos industriais específicos, como Modbus, DNP3 ou IEC 61850, e gerem exploits adaptados a cada ambiente com uma velocidade que nenhuma equipe humana consegue igualar.

Mas talvez o aspecto mais inquietante não seja a velocidade, e sim a sutileza. Modelos de machine learning podem analisar o comportamento de um sistema OT/IoT durante semanas ou meses, aprender seus padrões operacionais e desenvolver ataques que passem despercebidos pelos sistemas tradicionais de detecção. Uma pequena variação na pressão de uma tubulação. Uma variação imperceptível na frequência de uma turbina. Anomalias que nenhum operador humano detectaria a tempo.

O outro lado da IA: um escudo para a cibersegurança

No entanto, seria um erro reduzir o papel da inteligência artificial ao de mera ameaça. A mesma tecnologia que pode ser usada como arma por agentes maliciosos também é a ferramenta mais poderosa à disposição do setor para se defender.

Sistemas de detecção de anomalias baseados em IA podem monitorar, em tempo real, milhares de variáveis em um ambiente industrial, definir padrões de comportamento normal e emitir alertas diante de qualquer desvio, por menor que seja, antes que se transforme em um incidente.

A gestão de vulnerabilidades, a correlação de eventos em ambientes híbridos e a resposta automatizada a incidentes são áreas nas quais a inteligência artificial não apenas melhora a eficiência, mas pode ser o único meio viável de atuar na velocidade exigida pelos ataques mais sofisticados.

Um analista humano não consegue processar, em segundos, milhões de registros de um sistema SCADA. Um modelo bem treinado, sim.

O desafio que ninguém quer nomear

Mas há um problema estrutural que continua latente na indústria. Os ambientes OT simplesmente não foram projetados com a cibersegurança em mente. Muitos dos sistemas em operação têm décadas de uso, rodam em sistemas operacionais sem suporte, não contam com recursos de criptografia e não podem ser atualizados sem interromper processos de produção críticos. Integrar soluções de IA a esses ambientes é, tecnicamente, um enorme desafio. E, do ponto de vista cultural, as equipes de operações e de segurança ainda falam idiomas diferentes, com prioridades que muitas vezes entram em conflito.

Soma-se a isso a escassez de talentos especializados. Ainda há poucos profissionais que combinam conhecimento profundo de sistemas industriais, operação OT e cibersegurança, porque se trata de um perfil muito específico e de maturidade relativamente recente no mercado. Sem essa capacidade interna ou externa, até as soluções mais sofisticadas podem se transformar em caixas-pretas difíceis de gerenciar quando ocorre um incidente crítico.

Uma questão de prioridade estratégica

A proteção dos ambientes OT contra ameaças potencializadas por IA não pode continuar sendo um tema relegado aos departamentos técnicos. É uma questão de segurança nacional, continuidade econômica e responsabilidade social. Os ataques registrados nos últimos anos contra infraestruturas críticas, redes elétricas, plantas de tratamento de água ou sistemas de saúde não são fatos isolados, mas sinais claros de um risco crescente.

A resposta não pode chegar apenas depois que o ataque já ocorreu. A preparação precisa vir antes, com o cumprimento de marcos regulatórios que estabelecem requisitos mínimos de acordo com a criticidade do ambiente, investimento contínuo em formação especializada e colaboração real entre os setores público e privado, para além dos relatórios de boas intenções. A indústria tecnológica também precisa desenvolver soluções considerando a complexidade real dos ambientes OT/IoT, não apenas os cenários ideais e elegantes de laboratório.

A inteligência artificial chegou ao mundo industrial para ficar. A pergunta não é se transformará a cibersegurança OT, mas se seremos capazes de conduzir essa transformação antes que outros o façam em nosso lugar.

Luís Guillen
Cybersecurity Director

A primavera de 2026 não chegou sozinha

Cibercrônica por Alicia Isabel Martinez Vera

Enquanto a Europa começava a se preparar para o verão e as empresas aceleravam seus processos de digitalização, o espaço cibernético voltou a mostrar que não existem estações tranquilas. De meados de abril até hoje, o cenário da cibersegurança foi marcado pelo avanço de ransomwares cada vez mais agressivos, vazamentos massivos de dados e ataques a cadeias de suprimentos. Também ganhou força uma nova geração de ameaças impulsionadas por inteligência artificial.

A sensação predominante nas últimas semanas era clara: os cibercriminosos já não buscavam apenas roubar informações, mas paralisar operações, abalar a confiança e transformar a dependência digital em arma.

Durante o mês de abril, manteve-se uma tendência que já havia começado a se desenhar em 2025. Os provedores de tecnologia se consolidaram como o ponto de entrada preferido dos cibercriminosos. Relatórios de inteligência e análises setoriais alertaram para o aumento dos ataques direcionados a terceiros com acesso privilegiado a infraestruturas corporativas.

Um dos episódios mais simbólicos foi o ataque sofrido pela Inditex. A gigante têxtil confirmou o acesso não autorizado a bases de dados hospedadas em servidores de um provedor externo, reacendendo o debate sobre a segurança dos ecossistemas interconectados e a dificuldade de controlar riscos fora do perímetro corporativo.

Quase ao mesmo tempo, a rede de academias Basic-Fit sofreu uma invasão que acabou expondo dados pessoais de milhares de usuários europeus. Nomes, e-mails, telefones e dados bancários foram comprometidos em um dos ataques de maior repercussão no setor de varejo e serviços até aquele momento do ano.

Por trás desses incidentes, havia um padrão recorrente: os cibercriminosos nem sempre atacavam diretamente a vítima principal. O acesso ocorria por integrações esquecidas, aplicações conectadas ou fornecedores com defesas mais frágeis. O perímetro tradicional havia desaparecido definitivamente.

Outra tendência preocupante foi o uso massivo de inteligência artificial por agentes maliciosos.

Especialistas começaram a alertar que o phishing havia mudado para sempre. Os antigos e-mails cheios de erros ortográficos deram lugar a mensagens impecáveis, personalizadas e quase impossíveis de distinguir de uma comunicação legítima. A IA Generativa passou a ser usada para automatizar campanhas de engenharia social, clonar vozes e gerar mensagens hiper-realistas em larga escala.

Em paralelo, o ransomware evoluiu para modelos praticamente autônomos. Algumas campanhas detectadas em abril mostravam malware capaz de identificar sistemas críticos, criptografar informações e exfiltrar dados com mínima intervenção humana.

Depois de um abril marcado por incidentes corporativos, maio trouxe uma mudança de foco, com as administrações públicas voltando a ser alvo prioritário do ransomware.

O caso mais visível foi o da Prefeitura de Valdemoro. O município madrilenho sofreu um ataque que paralisou parcialmente serviços essenciais, afetando o cadastro municipal, sistemas de gestão e plataformas de pagamento.

Dias depois, veio a público que o grupo Kairos havia assumido a autoria da invasão e alegava ter obtido cerca de 1,8 TB de informações sensíveis. O incidente refletia uma tendência cada vez mais frequente: a “dupla extorsão”.

À medida que o mês avançava, ficou cada vez mais evidente que os vazamentos de dados haviam deixado de ser exceção. Dados publicados na Espanha mostraram que, durante 2025, foram reportados mais de 2.600 incidentes de segurança, afetando mais de 200 milhões de registros. A cifra equivalia, simbolicamente, a mais de quatro incidentes de segurança por cidadão. Os ataques já não afetavam apenas grandes multinacionais. Qualquer organização com dados, conectividade e dependência tecnológica podia se tornar alvo.

Enquanto os ataques aumentavam, a pressão regulatória também crescia. Durante abril, as instituições europeias reforçaram o debate sobre a aplicação da diretiva NIS2 e a necessidade de harmonizar obrigações de cibersegurança em toda a União Europeia.

Para sintetizar as últimas semanas em apenas uma ideia, poderíamos dizer o seguinte: a confiança digital se tornou o principal alvo dos cibercriminosos.

As empresas já não temem apenas perder dados; temem interromper operações, perder reputação e ver comprometida sua relação com clientes e parceiros. Os cibercriminosos aprenderam que o impacto psicológico e operacional pode ser tão valioso quanto o econômico.

Entre meados de abril e maio de 2026, ficou evidente que a cibersegurança havia entrado definitivamente em uma nova etapa. Uma fase na qual a IA ofensiva, o ransomware automatizado e a exploração de terceiros estão redefinindo o risco digital global.

Alicia Isabel Martinez Vera
Cybersecurity Consultant

Zero Trust e defesa em profundidade com ISA 62443

Artigo por Jhon Jaire Medina Davis

A cibersegurança das infraestruturas críticas já não pode depender apenas do perímetro. A convergência entre TI e OT, o telecontrole de instalações distribuídas, o acesso remoto de terceiros, os ativos legados e a exigência de continuidade do serviço obrigam as organizações a adotar modelos mais granulares e baseados em risco. Nesse cenário, o Zero Trust oferece um princípio valioso, eliminar a confiança implícita e verificar continuamente identidades, dispositivos, comunicações e acessos. No entanto, sua transferência direta da TI para OT é limitada por restrições de disponibilidade, determinismo, operação remota e ciclos de vida tecnológicos muito longos. Este artigo argumenta que a maneira mais eficaz de levar o Zero Trust ao ambiente industrial não consiste em replicar controles de TI, mas em integrá-lo à defesa em profundidade e materializá-lo por meio da metodologia ISA/IEC 62443. O texto explica a relação entre essas duas abordagens, seu vínculo com a segurança e a disponibilidade do processo, a cobertura oferecida pelos sete requisitos fundamentais da ISA/IEC 62443-3-3 e a importância da análise de riscos conforme a ISA/IEC 62443-3-2 para definir zonas, conduits, níveis-alvo de segurança e controles proporcionais. A abordagem é apresentada com uma linguagem especialmente próxima dos operadores, permitindo traduzir princípios estratégicos em medidas técnicas e organizacionais auditáveis, priorizadas e alinhadas à realidade operacional dos sistemas industriais.

As infraestruturas críticas operam sobre sistemas de automação e telecontrole cujo projeto histórico priorizou a segurança e a disponibilidade do processo, assim como a continuidade do serviço.

Durante anos, essa realidade favoreceu arquiteturas relativamente fechadas, com um número limitado de interconexões e fronteiras operacionais bem definidas. No entanto, a digitalização industrial, a conectividade com sistemas corporativos, o acesso remoto para operação e manutenção, a incorporação de análises avançadas e a necessidade de integrar dados operacionais a processos de negócio reduziram essa separação tradicional.

Em paralelo, o cenário de ameaças mudou. Hoje, a preocupação não se limita a ataques oportunistas, mas inclui campanhas direcionadas, ransomware com impacto operacional, abuso de acessos remotos, comprometimento de terceiros e movimentos laterais que exploram credenciais, redes planas e ativos com capacidades limitadas de proteção.

A premissa clássica de que “o que está dentro da rede de controle é confiável” já não se sustenta. Nesse contexto, o Zero Trust ganhou relevância como princípio orientador da cibersegurança moderna. No entanto, em OT, não pode ser implementado como uma cópia dos padrões da TI corporativa. O desafio não é importar um catálogo de tecnologias, mas reinterpretar seus princípios para um ambiente no qual um atraso de autenticação, uma varredura agressiva ou uma reinicialização não planejada podem resultar em perda de visibilidade do processo, manobras operacionais incorretas, degradação da qualidade ou interrupções do serviço.

A tese deste artigo é que a convergência prática entre Zero Trust e defesa em profundidade já está prevista na ISA/IEC 62443, desde que sua metodologia seja aplicada corretamente e com foco claro em risco.

Zero Trust em ambientes OT: princípios e limites de aplicação

O modelo Zero Trust parte de uma ideia simples. A confiança não deve ser implícita apenas porque um usuário, equipamento ou comunicação está dentro de uma determinada rede. A Cybersecurity and Infrastructure Security Agency (CISA) organiza essa abordagem em torno de pilares como identidade, dispositivos, redes, aplicações/cargas de trabalho e dados, apoiados por capacidades transversais de visibilidade, análise, automação e governança (CISA, 2023).

Por sua vez, o NIST destaca que o Zero Trust busca reduzir as zonas de confiança implícita, condicionar o acesso a processos granulares de autenticação e autorização e preservar a disponibilidade, `minimizando atrasos associados aos mecanismos de verificação (NIST, 2020).

A dificuldade surge quando esses princípios são aplicados ao ambiente OT. A própria CISA alerta que seu Zero Trust Maturity Model não aborda de forma específica os desafios associados a tecnologias operacionais, determinadas classes de IoT ou as restrições de dispositivos com opções limitadas de autenticação, visibilidade e segurança (CISA, 2023). Esse alerta é especialmente relevante em infraestruturas críticas, onde convivem PLCs, RTUs, HMIs, estações de engenharia, equipamentos de comunicação e ativos distribuídos com longa vida útil, suporte desigual e dependência de links de telecontrole.

Por isso, em ambientes OT, o Zero Trust deve ser entendido mais como um princípio de arquitetura e governança do que como um modelo uniforme de implementação. Nem sempre será viável instalar agentes, aplicar autenticação contextual contínua a todos os ativos ou exigir o mesmo nível de telemetria de uma rede de TI moderna.

Por outro lado, é viável eliminar a confiança implícita entre zonas, reforçar identidades humanas e de serviço, controlar rigorosamente o acesso remoto, limitar a conectividade ao estritamente necessário, exigir rastreabilidade, proteger a integridade das mudanças e usar controles compensatórios quando os ativos não permitem controles avançados. Em outras palavras, em ambientes OT, o Zero Trust não é implementado "da mesma forma que em TI". É implementado de forma adaptada, preservando o princípio e ajustando o mecanismo à criticidade e à operabilidade do processo.

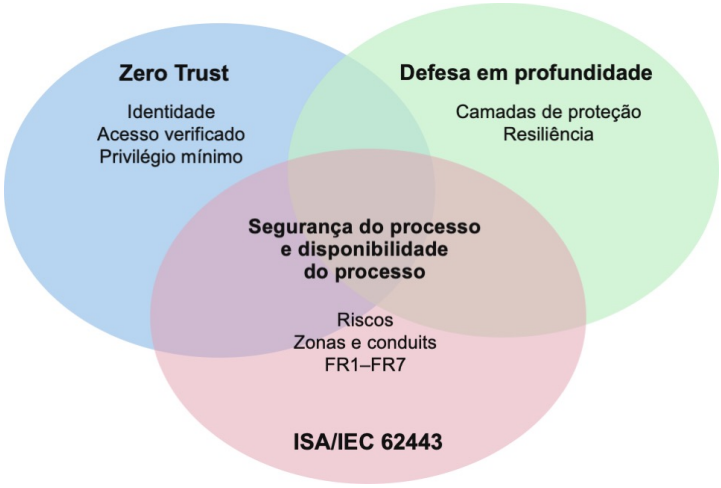


Figura 1: Convergência conceitual entre Zero Trust, defesa em profundidade e ISA/IEC 62443.

Defesa em profundidade e sua relação com a segurança e a disponibilidade do processo

A defesa em profundidade é especialmente adequada para infraestruturas críticas porque se alinha à forma como a segurança e a continuidade operacional do processo são tradicionalmente gerenciadas. Assim, como em uma análise de risco operacional, parte-se da premissa de que nenhuma medida de proteção isolada é suficiente para controlar cenários de alto impacto. O que torna o sistema robusto é a combinação de barreiras técnicas, operacionais e organizacionais. Em plantas de tratamento, estações de bombeamento, reservatórios, redes de distribuição e sistemas de saneamento, o risco não depende de um único equipamento ou de um único controle, mas da interação entre múltiplas medidas que precisam permanecer eficazes ao longo do tempo. A partir dessa perspectiva, a cibersegurança industrial converge naturalmente com a operação segura, ao buscar evitar que uma única falha, erro ou ação maliciosa comprometa a qualidade, a continuidade do serviço ou a integridade operacional do processo.

Em termos práticos, a defesa em profundidade em ambientes OT combina camadas de governança, proteção física de locais remotos, segmentação entre ambientes corporativos e operacionais, hardening de servidores e estações, proteção de PLCs, RTUs e dispositivos de campo, controle de acessos remotos de terceiros, monitoramento, resposta a incidentes e capacidades de backup e recuperação.

Seu objetivo não é apenas bloquear um acesso não autorizado, mas impedir que uma única fragilidade — por exemplo, uma conta compartilhada, uma estação de engenharia mal localizada, um gateway de telecontrole exposto ou uma DMZ permissiva — permita comprometer várias camadas ao mesmo tempo. A resiliência surge precisamente da combinação ordenada de barreiras e da independência relativa entre elas.

A relação com a segurança e a disponibilidade do processo é direta. Um incidente cibernético pode alterar setpoints, degradar a qualidade das informações, inibir alarmes, bloquear comunicações com estações remotas, modificar parâmetros operacionais ou impedir que as equipes atuem no momento necessário.

No setor de saneamento básico, isso pode resultar em dosagem incorreta de reagentes, manobras inadequadas de bombeamento, perda de visibilidade sobre reservatórios e estações, impactos na qualidade da água tratada ou interrupções no serviço. Por isso, em infraestruturas críticas, como de água e saneamento, a cibersegurança não deve ser considerada um domínio paralelo, mas uma condição necessária para preservar a operação dentro de seus limites previstos e manter a eficácia das barreiras técnicas e organizacionais do processo.

ISA/IEC 62443 como metodologia de implementação

O principal ponto forte da norma ISA/IEC 62443 é transformar conceitos estratégicos em uma metodologia aplicável. A série não se limita a uma lista de controles. Em vez disso, articula governança, análise de riscos, arquitetura e requisitos técnicos de forma coerente. Na parte 2-1, direcionada ao asset owner, a norma define o programa de segurança como a combinação de capacidades baseadas em processos, pessoas e tecnologia destinadas a reduzir o risco cibernético do IACS. A norma também reconhece que suas políticas devem conviver com as do ISMS corporativo sem perder de vista as restrições de disponibilidade e desempenho próprias do ambiente industrial (ISA, 2024).

A parte 3-2 funciona como uma ponte metodológica fundamental. A norma exige uma avaliação inicial do risco cibernético do sistema em questão, a divisão dos ativos em zonas e conduits de acordo com o risco e uma análise detalhada para determinar um Security Level Target (SL-T) para cada zona ou conduit (ISA, 2020).

Para operadores do setor de água e saneamento, isso significa partir da criticidade real de cada função de processo — por exemplo, captação, dosagem, bombeamento, armazenamento, distribuição ou telecontrole — e analisar quais consequências sua degradação teria para a segurança operacional, a qualidade da água, o compliance e a continuidade do serviço. A análise de cibersegurança não parte de uma visão abstrata, mas do conhecimento do processo e de suas consequências.

Por fim, a parte 3-3 estabelece os requisitos técnicos de sistema organizados em sete requisitos fundamentais. Essa estrutura facilita traduzir o SL-T em controles concretos, com granularidade suficiente para definir medidas realistas e auditáveis. Dessa forma, o Zero Trust oferece os princípios, a defesa em profundidade oferece a lógica de camadas e a ISA/IEC 62443 oferece o método para converter ambos em arquitetura, procedimentos, evidências e roteiro estratégico de melhoria.

Figura 2: Sequência recomendada para implementar controles de Zero Trust e defesa em profundidade por meio da ISA/IEC 62443.

Os sete requisitos fundamentais como uma estrutura para a convergência

A convergência entre Zero Trust e defesa em profundidade fica clara ao analisar os sete requisitos fundamentais da ISA/IEC 62443-3-3. A norma dialoga diretamente com o Zero Trust, pois já incorpora seus princípios essenciais ao exigir identificação robusta, privilégio mínimo, integridade, controle de fluxos, visibilidade e disponibilidade.

Ao mesmo tempo, a forma como esses requisitos se distribuem em zonas, conduits, funções e procedimentos os transforma em uma implementação natural da defesa em profundidade.

FR	Aporte ao Zero Trust	Aporte à defesa em profundidade	Exemplo típico em OT
FR1 IAC	Identidade verificada; autenticação forte; contas únicas; reforço de acessos remotos.	Primeira barreira frente a acessos não autorizados humanos ou de dispositivos.	Contas nominativas em SCADA e acesso remoto a ETAP/EDAR; MFA em telemanutenção.
FR2 UC	Privilégio mínimo, roles e segregação de funções.	Evita que uma mesma identidade possa escalar ou afetar várias camadas.	Roles diferenciados para operação central, manutenção, laboratório e fornecedores; controle de USB e portáteis.
FR3 SI	Verificação de integridade do sistema e de mudanças relevantes.	Reduz a probabilidade de alteração maliciosa ou acidental de ativos críticos.	Hardening, controle de configurações, proteção de PLC/RTU e validação de mudanças em consignas e firmware.
FR4 DC	Proteção de informação em trânsito e repouso segundo criticidade.	Adiciona uma camada de proteção sobre parâmetros, arquivos e acessos remotos.	Criptografia seletiva de acessos remotos, custódia segura de backups e arquivos de configuração.
FR5 RDF	Segmentação granular e conectividade mínima entre domínios de confiança.	Materializa zonas e conduits como barreiras arquitetônicas.	DMZ industrial, separação entre rede corporativa, rede de processo e telecontrole; regras por exceção.
FR6 TRE	Observabilidade, detecção e reação oportuna.	Adiciona camadas de detecção e contenção para reduzir permanência do atacante.	Monitoramento de rede OT, correlação de eventos e resposta a acessos anômalos ou perda de comunicações.
FR7 RA	Mantém resiliência e oferece suporte a decisões de acesso sem comprometer continuidade.	Assegura que o sistema continue operando ou possa se recuperar de forma segura.	Redundância, backups verificados, inventário, continuidade do serviço e recuperação de estações remotas.

Tabela 1: Relação entre os FR da ISA/IEC 62443, Zero Trust e defesa em profundidade

Em conjunto, os sete FR mostram que a ISA/IEC 62443 não obriga a escolher entre Zero Trust e defesa em profundidade. Pelo contrário, oferece uma linguagem comum para ambos. FR1 e FR2 materializam identidade e privilégio mínimo. FR3, FR4 e FR5 trazem integridade, proteção da informação e segmentação. FR6 e FR7 estendem a arquitetura para detecção, resposta e continuidade operacional. Essa cobertura é especialmente valiosa em ambientes OT porque evita abordagens parciais centradas apenas em firewalls ou autenticação. Também obriga a considerar simultaneamente controle de acesso, arquitetura de comunicações, integridade do sistema e resiliência.

A importância da análise de riscos e do SL-T

Uma das causas mais frequentes de fracasso em programas de cibersegurança industrial é tentar implementar controles antes de entender com precisão o risco que se deseja reduzir. A ISA/IEC 62443-3-2 ajuda a evitar esse erro ao exigir uma avaliação inicial do risco do sistema em questão, considerando o pior impacto não mitigado sobre segurança, meio ambiente, continuidade, produção, qualidade, finanças, compliance e reputação (ISA, 2020). No caso do setor de água e saneamento, essa análise também deve considerar efeitos concretos, como perda de controle sobre a dosagem, indisponibilidade do telecontrole, impacto na qualidade da água ou interrupção do serviço em estações remotas e plantas principais.

Essa abordagem se conecta de forma muito natural com HAZOP e LOPA. Na prática da análise de riscos operacionais, o valor não está apenas em listar ameaças, mas em compreender cenários, incluindo causas, desvios, consequências, medidas de proteção existentes, independência das camadas e risco residual. Transferida para a cibersegurança, a análise deve responder a perguntas como: o que aconteceria se uma estação de operação comprometida alterasse setpoints de dosagem? Qual seria o impacto da perda de comunicações com estações remotas de bombeamento ou reservatórios? O que ocorreria se um acesso remoto sem supervisão executasse manobras fora de sequência? Que camada seria perdida se a visibilidade do operador fosse degradada por malware ou pela indisponibilidade do historiador? Essa leitura permite identificar não apenas vulnerabilidades, mas necessidades exatas de redução de risco. A determinação do SL-T por zona ou conduit é uma consequência prática dessa análise.

Nem todas as zonas exigem o mesmo nível de rigor ou os mesmos controles. Uma rede de processo em planta, uma rede de telecontrole com estações remotas, uma DMZ industrial ou um servidor historiador podem compartilhar uma relação funcional, mas não o mesmo perfil de ameaça, criticidade ou tolerância a falhas. Quando o SL-T é definido corretamente, a organização evita tanto a subproteção quanto a sobreproteção.

Isso gera benefícios muito concretos, como a racionalização dos investimentos, a organização das fases de implementação e a melhoria do diálogo com operações e manutenção. Também permite justificar tecnicamente por que se exige MFA em um acesso remoto, por que se separam domínios de processo e telecontrole ou por que se reforça uma política de mídias removíveis.

Além disso, a norma exige documentar a análise de riscos e mantê-la como um ativo vivo para auditorias, testes, revisões futuras e evolução do design (ISA, 2020). Essa documentação constitui uma das maiores fortalezas da abordagem. Permite passar de decisões intuitivas para decisões demonstráveis. De “acreditamos que estamos protegidos” para “sabemos qual risco cada controle reduz e por que está onde está”.

Problemas recorrentes e benefícios de uma implementação correta

A experiência acumulada em avaliações de maturidade, revisão documental, visitas a plantas, análise de arquitetura e revisão técnica de configurações mostra padrões recorrentes.

Em instalações industriais, aparecem com frequência usuários genéricos em postos SCADA, credenciais expostas, estações de engenharia ou telecontrole atuando como pontes entre segmentos, regras de firewall excessivamente permissivas e DMZs industriais mal implementadas. Também são comuns acessos remotos de terceiros sem governança suficiente, uso não governado de USB, inventários desatualizados e diagramas de rede que não refletem o estado real da instalação. Nenhum desses problemas é extraordinário. Justamente por isso, são tão perigosos.

Quando a metodologia da ISA/IEC 62443 é aplicada corretamente, esses problemas deixam de ser tratados como incidentes isolados e passam a ser interpretados como sintomas de uma arquitetura sem limites de confiança bem definidos, sem atribuição correta de responsabilidades ou sem redução suficiente de risco.

Nesse momento, torna-se possível priorizar melhorias imediatas, como contas individuais, endurecimento de acessos remotos, reforço da DMZ, controle de portas, segmentação básica e centralização de logs. Ao mesmo tempo, a organização pode definir melhorias estruturais de médio prazo, como reestruturação por zonas e conduits, segregação entre redes corporativas, de processo e de telecontrole, governança do ciclo de vida de vulnerabilidades, procedimentos de backup/restore e exercícios de resposta a incidentes em OT.

O benefício não é apenas técnico. A abordagem também melhora a rastreabilidade, reduz a dependência do conhecimento tácito, facilita auditorias e organiza a relação entre TI e OT. Além disso, ajuda a liderança a decidir com mais clareza onde investir primeiro. Em outras palavras, o valor real da abordagem não está em acumular controles, mas em construir uma postura de segurança coerente com o processo e sustentável ao longo do tempo.

Problema observado	Risco dominante	Resposta prioritária alinhada à ISA 62443
Usuários genéricos em SCADA/HMI	Perda de rastreabilidade e facilidade de escalonamento.	FR1 e FR2: contas individuais, perfis de acesso, MFA quando aplicável e revisão de privilégios.
Estação de engenharia ou telecontrole usada como ponte entre segmentos	Movimento lateral, ponto único de falha e perda de controle do acesso.	FR5 e FR3: realocação da estação, segmentação de conduits e hardening do ativo.
DMZ industrial ou gateway de telecontrole permissivo	Acesso direto da TI a serviços OT críticos.	FR5 e FR1: regras por exceção, MFA, publicação de réplicas e registro de sessões.
Acesso remoto de terceiros sem controle suficiente	Manobras não supervisionadas, exposição de credenciais e baixa rastreabilidade.	FR1, FR2 e FR5: MFA, jump server, janelas de acesso e registro de sessões.
Uso de USB e dispositivos portáteis sem controle	Introdução de malware e alteração de configurações.	FR2, FR3 e FR7: política de mídias removíveis, validação prévia e procedimentos de varredura segura.
Inventários e diagramas desatualizados	Decisões de risco baseadas em uma arquitetura irreal.	ISA 62443-3-2 e 2-1: inventário confiável, documentação viva e revisão periódica de mudanças.

Tabela 2: Problemas recorrentes em avaliações OT e respostas recomendadas.

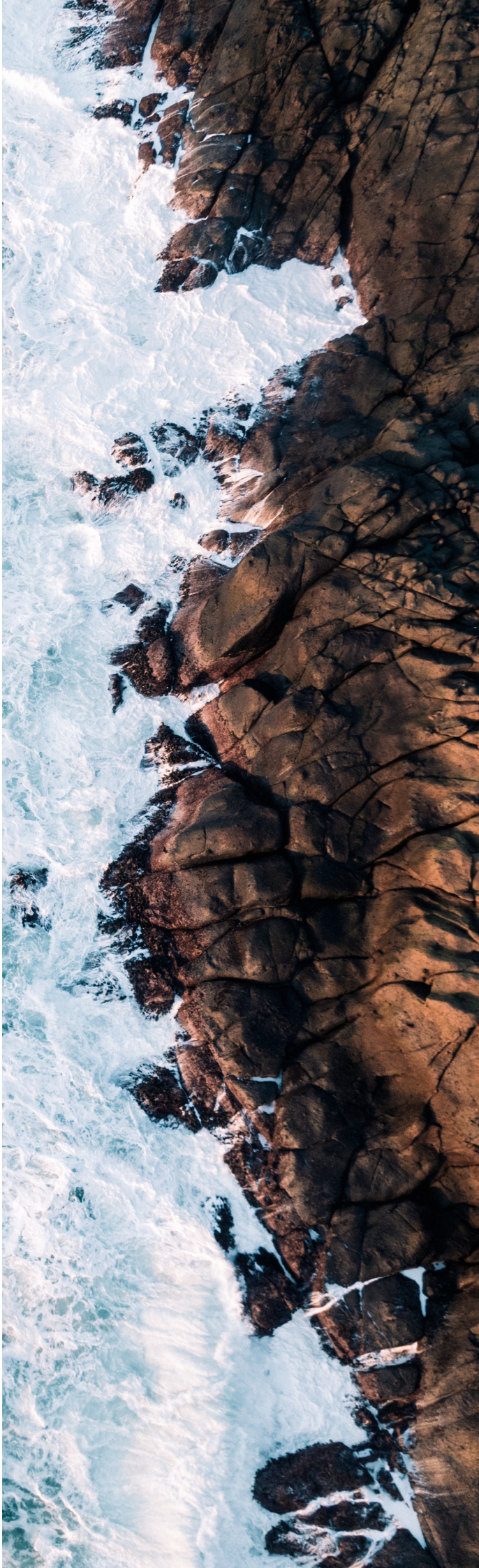
Conclusão

Zero Trust e defesa em profundidade não devem ser entendidos como abordagens alternativas para a proteção de infraestruturas críticas. O Zero Trust traz uma disciplina necessária ao questionar a confiança implícita, verificar cada acesso relevante e reduzir a conectividade ao estritamente necessário. A defesa em profundidade segue uma lógica bem conhecida no ambiente industrial. Nenhuma barreira isolada é suficiente, e a resiliência depende da combinação ordenada de camadas técnicas, físicas e organizacionais.

A ISA/IEC 62443 é a estrutura que permite integrar essas duas abordagens mantendo o alinhamento com a operação real de uma infraestrutura crítica. Seu valor está em conectar governança, análise de riscos, zonas e conduits, níveis-alvo de segurança e requisitos técnicos em uma metodologia verificável. Aplicada com rigor, a norma não apenas melhora a proteção cibernética do IACS, mas preserva a segurança e a disponibilidade do processo, favorece decisões de investimento baseadas em risco e transforma a cibersegurança industrial em uma disciplina auditável e gerenciável.

Para organizações do setor industrial, a mensagem é clara. A questão já não é se vale a pena incorporar princípios de Zero Trust, mas como fazer isso sem comprometer a disponibilidade, a continuidade do serviço ou a manutenibilidade. Na prática, a resposta consiste em adotar uma defesa em profundidade baseada em risco, com implementação orientada pela norma ISA/IEC 62443.

Jhon Jairo Medina Davis
Cybersecurity Technical Manager



Tendências OT: criptografia quântica em ambientes industriais

Tendências por Miren Ordoñez de Arce

Na cibersegurança industrial (OT), que envolve fábricas, plantas de energia e sistemas de transporte, a proteção das informações nunca foi tão crítica. À medida que a digitalização avança — com sensores, PLCs e redes industriais cada vez mais conectados — os riscos também aumentam. E, no horizonte, surge uma nova disrupção: a computação quântica.

Nesse cenário, a criptografia quântica ganha força como uma das tendências mais comentadas, com a promessa de redefinir a forma como protegemos as comunicações em ambientes industriais.

Por que a computação quântica preocupa tanto?

Hoje, a maioria dos sistemas de criptografia, como aqueles que protegem comunicações industriais ou redes corporativas, baseia-se em problemas matemáticos difíceis de resolver. No entanto, futuros computadores quânticos poderiam quebrar muitos desses sistemas em questão de minutos.

Isso cria um cenário preocupante para a indústria, em que dados de produção, receitas, configurações de máquinas e até infraestruturas críticas poderiam ficar expostos.

O que é exatamente a criptografia quântica?

Quando falamos em criptografia quântica, na prática nos referimos principalmente a uma tecnologia específica: a Distribuição Quântica de Chaves (QKD). De forma simples, a QKD permite que dois sistemas compartilhem uma chave secreta para criptografar informações usando princípios da física quântica, e não a matemática tradicional.

Isso tem uma consequência muito poderosa:

- Qualquer tentativa de interceptar a chave é detectada automaticamente pelo próprio sistema, porque medir um estado quântico altera seu comportamento.

Ou seja, além de proteger as informações, a tecnologia também alerta sobre intrusões em tempo real.

Como isso se encaixa em ambientes OT?

Embora possa parecer algo futurista, a criptografia quântica já está sendo explorada em cenários industriais reais. Por exemplo, seu uso já foi estudado em processos tão específicos quanto a transferência segura de programas para PLCs em fábricas.

Em ambientes OT, suas aplicações mais claras são:

- Proteção de comunicações entre plantas e centros de controle
- Segurança em redes de energia ou infraestruturas críticas
- Intercâmbio seguro de dados entre fornecedores e sistemas industriais

Isso é especialmente relevante porque muitos sistemas industriais têm ciclos de vida muito longos, de 10 a 20 anos, o que significa que precisam se preparar hoje para ameaças futuras.

Que vantagens oferece em relação à segurança tradicional?

A criptografia quântica traz uma mudança de paradigma:

- Segurança baseada na física, não na matemática. Não depende de um problema ser “difícil”, mas de leis físicas impossíveis de violar.
- Detecção de espionagem. Qualquer tentativa de interceptação deixa um rastro imediato.
- Preparação para o “Q-Day”. O momento em que os computadores quânticos poderão quebrar a criptografia atual.

Mas nem tudo é tão simples

Como toda tecnologia emergente, a criptografia quântica também apresenta desafios importantes:

- Custo e infraestrutura: requer hardware especializado e, em muitos casos, fibra óptica dedicada.
- Limitações de distância: a transmissão quântica ainda tem restrições técnicas.
- Integração com sistemas legados: algo especialmente complexo em OT.

Por isso, na prática, muitas organizações estão combinando QKD com outras soluções, como a criptografia pós-quântica baseada em software.

Moda ou realidade iminente?

Embora ainda não seja uma tecnologia massiva, a criptografia quântica já está saindo do laboratório. Embora ainda não seja uma tecnologia amplamente adotada, a criptografia quântica já está saindo dos laboratórios.

Projetos europeus como o EuroQCI e iniciativas industriais mostram que a tecnologia começa a se tornar uma prioridade estratégica, especialmente para setores críticos.

Conclusão: a segurança industrial entra em uma nova era

A criptografia quântica representa uma mudança profunda na forma como entendemos a cibersegurança. Para o mundo industrial, isso significa deixar de apenas proteger sistemas contra ameaças atuais e começar a se preparar para ameaças que ainda não chegaram.

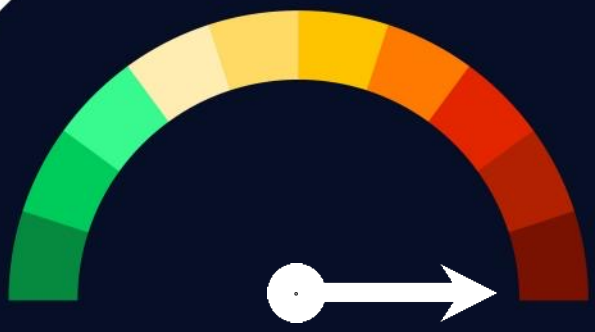
A criptografia quântica não substituirá as soluções atuais da noite para o dia, mas indica uma direção clara. A segurança do futuro será “quantum-safe” ou simplesmente não será.

Miren Ordoñez de Arce
Cybersecurity Lead Analyst

Vulnerabilidades

Vulnerabilidade de injeção SQL no MegaCMS da CRM Sistemas de Fidelización

Data: 29 de abril de 2026
CVE: CVE-2026-3325



CVSS: 10

CRÍTICA

Descrição

Foi descoberta uma vulnerabilidade de severidade crítica que afeta o MegaCMS, software usado para a gestão de sistemas de reservas, ticketing e venda on-line.

A vulnerabilidade ocorre devido à validação e sanitização inadequadas de um campo de entrada do usuário. Por meio de uma solicitação POST, o parâmetro 'id_territorio', utilizado imediatamente após o envio do formulário de registro, poderia ser manipulado por um invasor não autenticado para executar consultas SQL arbitrárias.

A vulnerabilidade já foi corrigida na versão mais recente do software, e a solução proposta é atualizar para essa última versão.

Solução

- O patch está incluído na versão mais recente disponível do software.
- Recomenda-se atualizar para a versão mais recente o quanto antes e monitorar tentativas de exploração nos logs dos servidores web.

Produtos afetados

- MegaCMS na versão 12.0.0.
- Alguns exemplos: sites de hotéis ou serviços turísticos, plataformas de eventos ou de venda de ingressos.

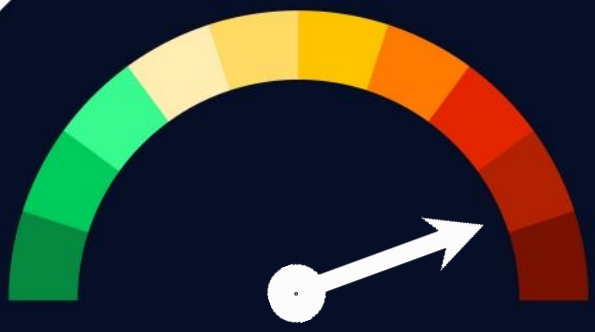
Referências

- incibe.es
- app.opencve.io

Vulnerabilidades

Integer Overflow no Blink/Google Chrome

Data: 6 de maio de 2026
CVE: CVE-2026-7896



CVSS: 8.8

ALTA

Descrição

Foi identificada uma vulnerabilidade crítica do tipo Integer Overflow no Blink, o motor de renderização utilizado pelo Google Chrome.

Essa vulnerabilidade ocorre durante o processamento de conteúdo HTML especialmente criado para exploração e pode provocar um integer overflow, levando à corrupção do heap.

Um agente remoto poderia explorar essa vulnerabilidade por meio de uma página web maliciosa, sem exigir interação adicional do usuário além de visitar ou abrir essa página com uma versão vulnerável do Chrome.

A exploração bem-sucedida poderia permitir a execução de código arbitrário no contexto do navegador afetado.

Solução

Recomendação:

- Atualizar o Google Chrome para a versão 148.0.7778.96/97 ou posterior, conforme o sistema operacional.

Produtos afetados

Alguns dos produtos afetados:

- Google Chrome para Windows, Linux e macOS anterior à versão 148.0.7778.96

Nota: outros navegadores baseados em Chromium poderiam ser impactados se incorporassem uma versão vulnerável do Blink, mas convém validar esse ponto nos avisos específicos de cada fabricante.

Referências

- app.opencve.io
- nvd.nist.gov
- chromereleases.googleblog.com

A Redis corrigiu falhas que permitiam execução de código em seus servidores

Data: 6 de maio de 2026
CVE: CVE-2026-23479 e outras 4

Alta

Descrição

A Redis identificou e corrigiu um total de 5 vulnerabilidades que permitiam a um invasor executar código remotamente em seus servidores.

A falha estava relacionada a diferentes vulnerabilidades de gestão de memória:

A CVE-2026-23479 e a CVE-2026-23631, vinculada ao Lua, permitiam a liberação de memória em uso (use-after-free), enquanto a CVE-2026-25243 possibilitava acessos inválidos por meio do comando RESTORE. Além disso, as CVE-2026-25588 e CVE-2026-25589 ampliavam esses riscos de execução de código para os módulos RedisTimeSeries e RedisBloom por meio do processamento de dados maliciosos.

Produtos afetados

- As cinco vulnerabilidades afetam as versões do Redis OSS/CE e Redis Software até a 8.0.6, inclusive.
- As versões corrigidas incluem Redis OSS/CE 6.2.22, 7.2.14, 7.4.9, 8.2.6, 8.4.3 e 8.6.3.
- No caso do Redis Software, as compilações corrigidas incluem 8.0.10-64, 7.22.2-79, 7.8.6-253, 7.4.6-279 e 7.2.4-153.

Solução

- Recomenda-se atualizar os módulos RedisTimeSeries para as versões v1.12.14, v1.10.24 ou v1.8.23, e RedisBloom para as versões v2.8.20, v2.6.28 ou v2.4.23.

Referências

- gbhackers.com
- nist.gov

Atualização do n8n corrige Prototype Pollution que pode levar a RCE

Data: 06 de maio de 2026
CVE: CVE-2026-42231

Crítica

Descrição

Foi lançada uma atualização de segurança do n8n para corrigir uma vulnerabilidade crítica que poderia permitir execução remota de código.

Trata-se de uma vulnerabilidade do tipo Prototype Pollution no tratamento de dados XML dentro do n8n, plataforma open source de automação de workflows baseada em Node.js. Essa vulnerabilidade permitiria que um usuário autenticado enviasse conteúdo XML especialmente criado para contaminar o protótipo global de objetos JavaScript.

A exploração bem-sucedida poderia permitir que o invasor encadeasse essa contaminação com outros nós da plataforma, como o nó Git e suas operações SSH, chegando à execução de código arbitrário no host afetado.

Produtos afetados

Os produtos afetados são:

- n8n em versões anteriores à 1.123.32
- n8n 2.17.x anterior à 2.17.4
- n8n 2.18.x anterior à 2.18.1

O aviso oficial identifica o pacote afetado como npm n8n.

Solução

Recomendação:

- Atualizar o n8n para 1.123.32, 2.17.4, 2.18.1 ou versões posteriores.

Referências

- incibe.es
- security.snyk.io

Eventos

Infosecurity Europe 2026
2 de junho – 4 de junho

A Infosecurity Europe 2026 será realizada de 2 a 4 de junho de 2026, em Londres, consolidando-se como um dos eventos de referência em cibersegurança na Europa. O encontro reunirá especialistas, CISOs, fabricantes de tecnologia e líderes da indústria para analisar ameaças emergentes, inteligência artificial aplicada à segurança, proteção de identidades digitais, Zero Trust e resiliência empresarial. O evento contará com mais de 300 expositores, workshops especializados e sessões técnicas voltadas à proteção de infraestruturas críticas e ambientes cloud.

Link

DES 2026 – Digital Enterprise Show
9 de junho – 11 de junho

O Digital Enterprise Show (DES) 2026 será realizado de 9 a 11 de junho em Málaga, reunindo mais de 15.000 executivos internacionais e líderes de tecnologia. Embora seja centrado em transformação digital e inteligência artificial, o evento terá um foco importante em cibersegurança, resiliência digital e proteção empresarial contra ameaças emergentes. Mais de 500 especialistas internacionais participarão do evento, abordando temas como segurança cloud, IA ofensiva, governança de dados e proteção de infraestruturas digitais.

Link

Cyb3rWall 2026
2 de junho – 4 de junho

O Congresso C1b3rWall 2026 será realizado de 2 a 4 de junho de 2026 na Escola Nacional de Polícia de Ávila, consolidando-se como um dos maiores encontros de cibersegurança e capacitação digital da Espanha. Organizada pela Polícia Nacional em parceria com a Universidade de Salamanca, esta sexta edição será realizada sob o tema “Cibercrimen 3.0”, reunindo especialistas nacionais e internacionais, forças e órgãos de segurança, empresas de tecnologia, universidades e profissionais da área de segurança digital.

Link

CCI – La Voz de la Industria Asturias
18 de junho

O Centro de Ciberseguridad Industrial realizará, em Gijón, o evento “La Voz de la Industria Asturias”, uma jornada especializada em cibersegurança industrial e proteção de infraestruturas críticas. O encontro reunirá especialistas em OT, responsáveis por segurança industrial e empresas dos setores de energia, manufatura e tecnologia para debater ameaças a ambientes industriais, continuidade operacional e regulação europeia em cibersegurança.

Link

Recursos

- **NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick Start Guide (QSG) – NIST**

Publicado pelo National Institute of Standards and Technology (NIST), este recurso oferece um guia prático para integrar a gestão de riscos de cibersegurança à estratégia global de gestão de riscos empresariais (ERM). O documento é voltado a responsáveis por segurança, executivos e equipes de governança corporativa que buscam alinhar a resiliência digital aos objetivos estratégicos do negócio. O guia aprofunda aspectos como governança de riscos, definição do apetite ao risco, gestão de riscos tecnológicos associados à IA, IoT, OT e cadeia de suprimentos, assim como a atribuição de responsabilidades organizacionais em cibersegurança. Trata-se de um recurso especialmente útil para organizações que adotam frameworks do NIST ou buscam adaptar seus programas de segurança a modelos mais maduros de gestão empresarial.

Link

- **The State of Cloud and AI Security 2025 – Cloud Security Alliance (CSA)**

Publicado pela Cloud Security Alliance (CSA) em colaboração com a Tenable, este relatório analisa como as organizações estão adaptando suas estratégias de segurança diante do crescimento acelerado de ambientes híbridos, multicloud e de inteligência artificial. Baseado em uma pesquisa global com mais de 1.000 profissionais, o documento identifica as principais lacunas entre adoção tecnológica e maturidade em cibersegurança. O relatório aborda riscos associados à IA Generativa, gestão de identidades, proteção de dados em cloud, exposição de configurações incorretas e automação de ameaças. Além disso, oferece recomendações práticas para fortalecer a resiliência organizacional e melhorar a visibilidade sobre superfícies de ataque cada vez mais complexas.

Link

- **CIS Critical Security Controls v8 – Center for Internet Security (CIS)**

Os CIS Controls v8 constituem um conjunto de melhores práticas priorizadas para ajudar organizações a prevenir, detectar e responder a ameaças cibernéticas. O framework foi desenvolvido para oferecer controles práticos e mensuráveis, que permitam reduzir riscos de forma progressiva e efetiva. O guia inclui recomendações sobre gestão de ativos, proteção de identidades, monitoramento contínuo, hardening de sistemas, segurança cloud, resposta a incidentes e treinamentos de conscientização. Sua abordagem prática e escalável faz dele um dos padrões mais usados por empresas e órgãos públicos para estruturar programas de cibersegurança.

Link

Inscreva-se na RADAR
up.nttdata.com/suscribetearadar

Powered by the Cybersecurity NTT DATA Team

br.nttdata.com