Mantendo os serviços públicos em funcionamento

É importante proteger a infraestrutura de energia elétrica, água, gás natural e energias renováveis.

Os riscos

Os serviços públicos fazem muito mais do que só manter as empresas de pé. Eles mantêm os hospitais em funcionamento com energia de reserva, a água potável, o gás nas residências durante o inverno e os serviços de emergência em funcionamento. Quando um serviço público falha, ele não falha sozinho. Outros setores também são afetados.

Grupos ligados a governos demonstraram que o objetivo é a interrupção, não o roubo de dados. O Volt Typhoon passou 300 dias sem ser detectado dentro de uma concessionária de água e eletricidade nos EUA, realizando o mapeamento dos procedimentos operacionais de tecnologia operacional (OT) e da topologia da rede.[1] O FBI e a CISA confirmaram que o padrão não é isolado: as concessionárias se tornaram um alvo principal para agentes ligados a governos, grupos de ransomware e ataques destrutivos.

Essa interrupção tem maior probabilidade de ocorrer em uma subestação remota, uma estação de bombeamento de água ou uma usina de geração de energia rural, onde não há profissionais de TI no local e o especialista mais próximo pode estar a horas de distância. A janela de tempo para restabelecer a energia, a pressão da água ou o fluxo de gás para uma comunidade é medida em minutos, não em dias úteis.

A lição das empresas de água americanas

Em 2024, a maior concessionária de água dos EUA sofreu um ataque cibernético que não afetou os sistemas operacionais, mas forçou a suspensão da cobrança e o fechamento do portal. Os sistemas de TI dos quais a OT depende, incluindo o Active Directory, historiadores de dados, GIS, OMS e faturamento, estão igualmente em risco.[2]

[1] https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days

[2] https://www.amwater.com/press-room/press-releases/corporate/american-water-reactivating-systems-after-cyber-event-10102024

Copyright © 2003-2026 Acronis International GmbH.

O cenário de ameaças

Uma em cada cinco organizações de ICS/OT sofreu um incidente cibernético confirmado no último ano. Não são alertas. Os incidentes confirmados afetaram os sistemas operacionais, sendo que 40% causaram interrupção operacional direta e quase um em cada cinco levou mais de um mês para ser solucionado. Para as concessionárias, essa lacuna de remediação não é apenas uma estatística. São dias sem fornecimento confiável de energia elétrica, água ou gás para as comunidades que dependem desses serviços.

Uma em cinco

organizações de ICS/OT sofreram um incidente cibernético no último ano.

Estado da Segurança ICS/OT da SANS em 2025

40%

de interrupção operacional, afetando produção, prestação de serviços ou operações públicas. 37,9% originaram-se de ransomware.

Estado da Segurança ICS/OT da SANS em 2025

19%

dos incidentes de OT levaram mais de um mês para serem recuperados em 2025. A detecção melhorou. A restauração continua sendo a lacuna crítica.

Estado da Segurança ICS/OT da SANS em 2025

As pequenas e médias concessionárias são descritas como cheias de alvos, mas pobres em cibersegurança: alvos de alto valor sem equipes dedicadas à cibersegurança e com recursos limitados para recuperação.

A solução: recuperação que funciona onde sua equipe não está presente

O Acronis Cyber Protect for OT oferece resiliência cibernética de nível de TI para ambientes OT de concessionárias, sem interromper as operações em tempo real. Ele foi desenvolvido com base em uma realidade operacional fundamental: quando ocorre um incidente em uma subestação remota, estação de bombeamento ou instalação de energia, a pessoa mais próxima do sistema pode ser um engenheiro de automação ou supervisor de turno, e não um especialista em cibersegurança. Os fluxos de trabalho de recuperação são criados para serem executados localmente por essas pessoas, com dependência mínima de conectividade externa ou intervenção especializada.

Backup sem interrupção
Backup completo de imagem e backup no nível do arquivo sem reinicializações e sem tempo de inatividade. O modo setor por setor é ativado automaticamente para sistemas de arquivos OT proprietários. Instantâneos consistentes com VSS em configurações SCADA e de historiadores de dados de vários volumes.

Restauração bare metal e universal
Recuperação automática para hardware diferente ou de substituição. A restauração universal injeta os drivers corretos sem reconfiguração manual, o que é fundamental quando o PC industrial original está obsoleto ou indisponível.

Operação isolada e off-line
Todos os componentes são implantados localmente. O servidor de gerenciamento funciona totalmente off-line. As definições de antimalware são atualizadas sem acesso à internet e os agentes continuam a proteção por 30 dias se o servidor de gerenciamento estiver inacessível.

Operação de recuperação com um clique para operadores
Pessoal autorizado no local, incluindo engenheiros de subestação, gerentes de operações de água e supervisores de turno, pode seguir um fluxo de trabalho de recuperação guiado para restaurar um sistema com falha ao seu último estado funcional conhecido, ajudando a reduzir o tempo de recuperação de horas ou dias para minutos, dependendo das condições no local.

Recuperação segura e verificada
As imagens de backup são verificadas em busca de malware e validadas antes da restauração, ajudando a reduzir o risco de reinfecção de um sistema SCADA ou HMI recuperado. As ameaças detectadas são sinalizadas e podem ser removidas como parte do fluxo de trabalho de recuperação.

Armazenamento de backup imutável
Os arquivos de backup não podem ser excluídos, modificados ou criptografados por ransomware, mesmo que as credenciais sejam comprometidas. Modos de governança e conformidade com períodos de retenção de até 10 anos para exigências regulatórias.

Copyright © 2003-2026 Acronis International GmbH.

Sistemas legados: protegendo o que outros abandonaram

Os ativos de OT de concessionárias operam por 30 anos ou mais. Os sistemas computadorizados que os gerenciam, incluindo IHMs, servidores SCADA e estações de trabalho de engenharia, geralmente executam sistemas operacionais que os principais fornecedores deixaram de oferecer suporte há anos.

Windows 10 em OT: gerenciando o risco do ciclo de vida[3]

Muitas estações de trabalho de OT de concessionárias ainda executam edições do Windows 10 com diferentes cronogramas de suporte. Algumas já estão fora de suporte, enquanto outras enfrentam marcos de ciclo de vida em 2027, 2029 ou posteriormente. Atualizar ou aplicar patches nesses sistemas geralmente não é uma tarefa rotineira; pode desencadear uma revalidação dispendiosa, quebrar o software SCADA/HMI licenciado ou invalidar contratos de suporte do fabricante original. A Acronis atua como um controle compensatório, combinando backup em imagem com a criação de listas de permissão de aplicativos para ajudar a operar sistemas legados com mais segurança quando a migração imediata do sistema operacional não é viável.

A Acronis oferece amplo suporte para backup completo e recuperação do Windows XP SP1/SP2/SP3 até o Windows Server 2025, kernel Linux 2.6.9 a 5.19 e todos os principais hipervisores, abrangendo todas as gerações de OT.

Recuperação e restauração: não são a mesma coisa

Em ambientes de concessionárias, confundir esses dois termos compromete a continuidade do serviço e, nos piores casos, a segurança pública.

Recuperação significa restabelecer o controle de frequência ou a pressão da água a partir de qualquer estado validado disponível, rapidamente. Operações parciais que mantêm um hospital em funcionamento não são um estado de falha. São a primeira missão.

Restauração significa devolver toda a pilha de sistemas certificados a um estado base conhecido e funcional de forma segura, sem reintroduzir malware ou corrupção.

A Acronis oferece suporte a ambos. A recuperação com um clique ajuda a garantir a continuidade operacional rápida, permitindo que o pessoal autorizado inicie a restauração localmente sem intervenção de especialistas. O backup validado e de nível forense oferece suporte à restauração completa e verificada, incluindo a verificação de imagens de backup em busca de malware antes do uso e o fornecimento de evidências de cadeia de custódia autenticadas por blockchain para investigação e auditoria pós-incidente.

De acordo com o relatório SANS State of ICS/OT Security 2025, embora quase metade dos incidentes de OT sejam detectados em 24 horas, 19% levam mais de um mês para serem totalmente restaurados. A detecção melhorou. A restauração continua sendo a lacuna crítica.

[3] https://learn.microsoft.com/en-us/windows/release-health/release-information

Copyright © 2003-2026 Acronis International GmbH.

O que a Acronis protege em toda a infraestrutura de serviços públicos

Ambiente de concessionárias	Sistemas e dados que a Acronis protege
Energia elétrica: geração, transmissão e distribuição, borda da rede	Servidores SCADA/EMS, PCs de controle de subestações, estações de trabalho HMI, controladores de DER/microrredes, controladores de sites BESS e servidores historiadores de dados. Os dados protegidos incluem imagens de SO, configurações SCADA/HMI, lógica de alarme, bancos de dados historiadores e arquivos de projetos de engenharia.
Água e esgoto	Sistemas SCADA para tratamento de água, estações de trabalho HMI, PCs de controle de estações elevatórias e de bombeamento, sistemas de monitoramento de reservatórios. Os dados protegidos incluem imagens de SO, configurações de processos de tratamento, lógica de controle de bombas e dados de relatórios regulatórios.
Distribuição de gás natural	Servidores de monitoramento de dutos, PCs de estações de compressão, PCs de estações reguladoras, servidores SCADA, sistemas de transferência de custódia. Os dados protegidos incluem configurações de processos, dados de monitoramento, arquivos de calibração e registros operacionais de dutos.
Energia renovável: eólica, solar, hídrica, biomassa e hidrogênio verde	PCs de controladores de turbinas/inversores, servidores de gerenciamento de plantas, sistemas de gerenciamento de BESS, monitoramento ambiental. Os dados protegidos incluem software de controle, configurações de instalações e conjuntos de dados operacionais.
Sistemas de TI dos quais a OT depende	Active Directory/DNS, jump hosts, historiadores de dados (parte de TI), GIS, OMS, AMI/MDMS, portais de faturamento e de clientes. Os dados protegidos incluem imagens de sistemas, dados de configuração, registros de clientes e operacionais.

Integração com SIEM: a integração da Acronis com SIEMs locais encaminha alertas de backup, segurança e RMM para SIEMs de terceiros via syslog, ajudando as equipes de OT e segurança a centralizar a visibilidade de incidentes em todos os ambientes protegidos.

Copyright © 2003-2026 Acronis International GmbH.

Conformidade e garantia

A Acronis auxilia as concessionárias a gerar evidências de planos de recuperação e registros de validação de backup, restaurar resultados de testes e controles de retenção, além de garantir a documentação de certificação de fornecedores que pode dar suporte à preparação para auditorias em estruturas importantes. A Acronis tem certificação IEC 62443-4-1.

NERC CIP (América do Norte)

Pode ajudar a fornecer evidências para a documentação do plano de recuperação CIP-009 por meio de registros de validação de backup e dados forenses de backup. Projetado para operar em redes totalmente isoladas, sem dependência da nuvem.

Diretiva NIS 2 (Europa)

Pode contribuir para as expectativas do Artigo 21 relativas à continuidade dos negócios e à gestão de backups. Cópias de segurança imutáveis e períodos de retenção configuráveis estão em consonância com a intenção do NIS 2 de proteção de dados e preparação para recuperação.

IEC 62443 (global)

Certificado IEC 62443-4-1 SSDLC. Backups em tempo real e sem interrupções, bem como a verificação de integridade, estão alinhados às expectativas de disponibilidade de recursos e continuidade dentro da estrutura da norma IEC 62443.

Lei de Ciber-resiliência da UE

A certificação do ciclo de vida de desenvolvimento seguro pode dar suporte às avaliações de garantia de fornecedores OEM, cada vez mais exigidas nas aquisições de serviços públicos no âmbito da CRA da UE.

Observação: a Acronis oferece suporte à comprovação do plano de recuperação e à preparação para auditorias. O cumprimento de qualquer quadro regulamentar continua sendo da responsabilidade do operador.

Parceiros e integradores OEM

O Acronis Cyber Protect for OT está disponível como solução white label, com marca compartilhada ou vendida como referência, permitindo que parceiros OEM e integradores de sistemas de controle incorporem a resiliência cibernética de OT diretamente em seus portfólios de sistemas de serviços públicos.

A Acronis trabalha com OEMs e parceiros de tecnologia industrial em ambientes de OT globalmente, incluindo ABB, Emerson, GE Vernova, Honeywell, Rockwell Automation, Schneider Electric e Yokogawa.

Copyright © 2003-2026 Acronis International GmbH.

Para parceiros OEM

- Incorpore a recuperação com um clique nativamente. Seja um parceiro de resiliência, não apenas um fornecedor de hardware.
- Ajude a reduzir o volume de chamadas de suporte reativo e os custos de deslocamento de engenheiros para cenários comuns de recuperação.
- Habilite serviços recorrentes de resiliência gerenciada e aumente a receita de contratos.
- Certificado pela norma IEC 62443-4-1, cada vez mais decisiva em licitações de concessionárias e na conformidade com a Lei de Ciber-resiliência da UE (CRA).

Para integradores de sistemas de controle

- Inclua a recuperação como parte da entrega do servidor SCADA/HMI/OT.
- Padronize os procedimentos de restauração em todos os sistemas de concessionárias entregues.
- Reduza a carga de suporte pós-implantação e a responsabilidade pelo SLA.
- Adicione serviços de resiliência recorrentes aos portfólios de projetos e serviços gerenciados.
- Venda por referência ou faça co-branding com sua equipe de integração.

Pronto para proteger a infraestrutura da qual as comunidades dependem?

Converse com um especialista em OT da Acronis ou com seu parceiro OEM para agendar uma demonstração ao vivo.

FALE COM UM ESPECIALISTA EM OT

Acronis

Saiba mais em
www.acronis.com

Copyright © 2003-2026 Acronis International GmbH. Todos os direitos reservados. A Acronis e o logotipo da Acronis são marcas comerciais da Acronis International GmbH nos Estados Unidos e/ou em outros países. Quaisquer outras marcas comerciais ou registradas são propriedade de seus respectivos donos. Pode haver alterações técnicas e diferenças em relação às ilustrações, bem como erros. 2026-07