Valor
R$ 5,00
(unitário)

cidadeseminerais.com.br

Cidades & Minerais

NOTÍCIAS DA MINERAÇÃO, DA SIDERURGIA E DOS MUNICÍPIOS.

EDIÇÃO 11 - MARÇO DE 2026

Quando o sistema cai, o prejuízo se multiplica

Ataques cibernéticos avançam no Brasil, pressionam empresas e poder público e colocam a segurança digital no foco das atenções

VALNET

Páginas 06 à 09

Vale até 2053:

o fôlego e o alerta

Extensão de 12 anos no horizonte da mineração alivia a economia e reduz a pressão imediata, mas reforça um recado incômodo: Itabira ganhou tempo, não solução

Páginas 02 e 03

Guanhães

no radar de novos investimentos

Páginas 10 e 11

Cibersegurança

Quando o sistema cai, o prejuízo se multiplica

Ataques cibernéticos avançam no Brasil, pressionam empresas e poder público e colocam a segurança digital no foco das atenções

VALENET

A digitalização deixou de ser tendência para se tornar espinha dorsal da operação empresarial e dos serviços públicos no Brasil. Na mineração, por exemplo, atividade carro-chefe da economia em Minas Gerais, sensores, sistemas de monitoramento de barragens, ERPs, telemetria e comunicação entre unidades remotas sustentam decisões em tempo real. No setor público (prefeituras, câmaras e outros órgãos governamentais), folha de pagamento, emissão de notas, protocolos eletrônicos, sistemas de saúde e portais de transparência funcionam em rede. Quando essa engrenagem falha, o impacto é imediato: produção interrompida, serviços suspensos, dados expostos e reputações colocadas em xeque.

Relatórios recentes de empresas de cibersegurança, como Fortinet, FortiGuard Labs, CTIR Gov e Brasscom, indicam que o Brasil concentrou cerca de 314,8 bilhões de tentativas de ataques cibernéticos apenas no primeiro semestre de 2025 — 84% de todas as ocorrências registradas na América Latina e Canadá. O número ajuda a explicar por que o tema deixou de ser pauta exclusiva de bancos e grandes corporações: órgãos públicos e empresas de todos os portes também entraram no radar do crime digital.

O custo da indisponibilidade também subiu. Estudos internacionais estimam perdas médias de até US$ 306 mil por hora em grandes operações. Mesmo empresas médias acumulam prejuízos significativos a cada hora de sistema parado. No setor público, além do impacto financeiro, há desgaste político e quebra de confiança, um fator ainda mais sensível em cidades onde a reputação institucional é construída no cotidiano. Segurança digital, portanto, não é acessório tecnológico. É requisito operacional.

Da conexão rápida à infraestrutura resiliente

Durante anos, a discussão, de modo geral, girou em torno da velocidade da internet. A lógica atual é diferente: não basta ter banda larga. É necessário que a conexão já venha estruturada com camadas de proteção, redundância física e lógica, monitoramento contínuo e plano de recuperação de desastres.

Nesse contexto, a infraestrutura requerida pelos mais diferentes organizações, tanto públicos quanto privados, é ampla. O firewall de nova geração (NGFW), sigla em inglês para Next Generation Firewall, por exemplo, funciona como uma "barreira inteligente" capaz de identificar e bloquear ameaças avançadas.

A proteção anti-DDoS, por sua vez, impede ataques de sobrecarga que tentam derrubar sistemas ao inundá-los com acessos simultâneos (imagine um concorrente desleal que queira tirar uma loja virtual do ar).

A VPN com arquitetura ZTNA — rede privada virtual baseada no conceito de "confiança zero" — verifica cada acesso individualmente antes de liberá-lo, com base nos "hábitos" do usuário.

Já o backup em nuvem, com testes periódicos de restauração, garante que cópias de segurança armazenadas fora do ambiente físico possam ser recuperadas quando necessário.

Dentre outras soluções, complementam essa estrutura as redes privadas como MPLS (Multiprotocol Label Switching), tecnologia que prioriza e organiza o tráfego de dados, e SD-WAN (Software-Defined Wide Area Network), rede inteligente que gerencia diferentes conexões de forma automática. São recursos que passaram a integrar o vocabulário das áreas de TI e, cada vez mais, das diretorias executivas.

Embora pareça algo complicado, tudo fica mais fácil quando o parceiro de negócios é um provedor de soluções em serviços customizados em tecnologia de última geração, como a Valenet Empresas. Com sede em Itabira e presença em mais de 120 localidades mineiras, a companhia evoluiu de provedora de conectividade para integradora de infraestrutura digital segura, com quase 20 mil quilômetros de rede própria 100% fibra óptica e suporte 24 horas por dia.

A empresa estrutura projetos com backbone dedicado, topologias em malha para reduzir pontos únicos de falha, IP válido, links redundantes e monitoramento 24x7. O objetivo é antecipar incidentes antes que o usuário final perceba qualquer impacto.

O porta-voz técnico da Valenet Empresas e especialista em redes e cibersegurança, Carlos Peres, afirma que o assunto é da mais alta relevância para as empresas e órgãos públicos. “Vivemos a era da digitalização inteligente, onde operações e serviços públicos essenciais dependem de sistemas conectados. Essa conectividade traz eficiência, economia e transparência, mas também aumenta o risco de ameaças cibernéticas que podem paralisar serviços e expor dados sensíveis”, afirma.

Segundo o especialista, a mudança é estratégica: sair da lógica reativa e migrar para um modelo preventivo, no qual indisponibilidade não é tratada como eventualidade aceitável.

Mineração conectada:

produção, segurança e dados no mesmo eixo

No âmbito da mineração, a conectividade sustenta não apenas produtividade, mas segurança operacional. Minas remotas dependem de comunicação constante com centros administrativos, controle de equipamentos e transmissão de dados críticos. Logo, uma falha pode interromper operações, atrasar decisões e ampliar riscos.

Entre os clientes atendidos pela Valenet Empresas neste universo está a Jaguar Mining, que implantou 19 quilômetros de fibra óptica dedicada para interligar unidades rurais à matriz em Belo Horizonte. Fibra dedicada significa uma conexão exclusiva para a empresa, sem compartilhamento com outros usuários, o que garante maior estabilidade e velocidade constante, mesmo em picos de uso.

A infraestrutura inclui também backbone próprio — rede principal que concentra e distribui todo o tráfego de dados da operação —, firewall em alta disponibilidade (dois equipamentos funcionando em paralelo para que, se um falhar, o outro assuma automaticamente) e VPN segura, que permite acesso remoto criptografado aos sistemas internos.

Na prática, todo esse aparato possibilita acompanhamento remoto de equipamentos, integração de telefonia corporativa e atualização em tempo real de indicadores estratégicos, reduzindo risco de paralisações, aumentando a segurança operacional e evitando prejuízos decorrentes de falhas ou ataques cibernéticos.

Em operações de grande escala, em que cada hora parada impacta contratos e produção, esse tipo de investimento deixa de ser custo de TI e passa a ser mecanismo direto de proteção do faturamento e da própria continuidade do negócio.

Outras empresas, como AngloGold Ashanti, ArcelorMittal e RHI Magnesita, também integram o portfólio B2B da Valenet Empresas, cases que reforçam a presença da companhia em cadeias produtivas estratégicas do estado de Minas Gerais.

Carlos Peres,
Gerente Comercial B2B de Grandes Contas da Valenet Empresas

Gestão pública: serviços essenciais não podem sair do ar

No universo da administração pública, a lógica é parecida. A digitalização das prefeituras, por exemplo, ampliou a eficiência administrativa, mas também elevou o grau de exposição. Sistemas tributários, saúde, educação e protocolos internos operam de forma integrada, o que é ótimo para o contribuinte, mas também aumenta as preocupações com a segurança digital.

Afinal, uma invasão por ransomware — tipo de ataque em que criminosos digitais sequestram os sistemas da instituição, criptografam os arquivos e exigem pagamento de resgate para devolver o acesso — pode paralisar serviços, atrasar pagamentos, bloquear completamente bancos de dados e comprometer informações pessoais de milhares de cidadãos.

Um case que vale destaque é o da Câmara Municipal de Itabira. Devido aos frequentes incidentes de interrupção de energia na cidade, os servidores da Casa Legislativa sofriam danos recorrentes, impactando diretamente a disponibilidade dos serviços.

Segundo o consultor de TI da Câmara, Marcelo Pires Guerra, em situações mais críticas, era necessário reinstalar sistemas operacionais, refazer todas as configurações, parametrizações e, somente depois, restaurar os dados existentes na nuvem.

“Com a implantação da solução Veeam Backup, apresentada pela Valenet Empresas, houve uma mudança significativa nesse cenário. A nova plataforma elevou consideravelmente o nível de segurança da informação e reduziu de forma drástica o tempo de recuperação de desastre, graças aos seus recursos avançados de backup e restauração de máquinas virtuais completas”, disse o consultor.

“De forma quase imediata após a implantação, enfrentamos um novo episódio de queda de energia que ocasionou a perda de diversos discos rígidos dos servidores. Foi nesse momento que o investimento mostrou todo o seu valor: utilizando os recursos do Veeam Backup, conseguimos restaurar todo o ambiente de rede de forma rápida, segura e com muito menos impacto operacional”, relatou.

LGPD, contratos e reputação

Segurança digital está intimamente relacionada também à legislação no que diz respeito às informações pessoais. Desde a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), manter os dados seguros tornou-se obrigação legal de empresas e instituições.

A legislação exige medidas técnicas e organizacionais adequadas para evitar acessos não autorizados, vazamentos e incidentes de segurança. As penalidades incluem multas de até 2% do faturamento, podendo alcançar R$ 50 milhões por infração.

Mais do que sanções financeiras, no entanto, o impacto reputacional costuma ser o fator mais sensível. Empresas que sofrem vazamentos enfrentam auditorias rigorosas, perda de contratos e questionamentos de parceiros. No setor público, a consequência pode ser desgaste político e desconfiança institucional.

Brasil ocupa a primeira posição na América Latina em ataques ransomware

Estrutura, capilaridade e suporte

Com mais de 25 anos de atuação, presença em mais de 120 localidades, cerca de 20 mil quilômetros de rede própria 100% fibra óptica, 1.300 colaboradores diretos e suporte 24 horas por dia, a Valenet Empresas consolidou estrutura capaz de atender desde hospitais e câmaras municipais até operações empresariais de grande porte.

A lógica adotada não se limita à venda de link dedicado. O modelo integra conectividade, firewall, backup em nuvem, comunicação unificada, Wi-Fi corporativo segmentado e monitoramento contínuo com SLA personalizado.

No ambiente empresarial mineiro — historicamente marcado por prudência na escolha de fornecedores —, reputação e proximidade contam tanto quanto tecnologia. Nesse aspecto, a presença física da empresa em Itabira e Belo Horizonte, aliada à capilaridade regional, contribui para respostas mais rápidas e relacionamento contínuo com gestores públicos e privados.

A digitalização é irreversível. A exposição, também. No cenário atual, proteger dados significa proteger produção, arrecadação, empregos e serviços essenciais. Para mineração e gestão pública em Minas Gerais, a segurança digital deixou de ser um debate técnico restrito à TI. Passou a integrar a agenda estratégica de quem decide e de quem precisa manter o sistema funcionando todos os dias.

Prudência digital: um checklist mínimo

Diante de um cenário em que a digitalização avança mais rápido que a cultura de prevenção, especialistas defendem que empresas e órgãos públicos adotem um conjunto mínimo de medidas estruturantes para reduzir vulnerabilidades e garantir continuidade operacional. Não se trata de luxo tecnológico, mas de um pacote básico de proteção capaz de evitar paralisações, vazamentos de dados e prejuízos financeiros e institucionais.

Para mineradoras e órgãos públicos, especialistas recomendam ao menos:

- Firewall de nova geração em alta disponibilidade.
- Backup em nuvem com testes periódicos de restauração.
- Segmentação entre redes administrativas e redes abertas.
- Redundância de links físicos com rotas distintas.
- Monitoramento 24x7 com resposta estruturada a incidentes.
- Política formal de acesso remoto com VPN segura.
- Plano documentado de continuidade de negócios.
- Treinamento recorrente contra phishing e engenharia social.