Considerações e soluções para o ambiente de trabalho digital do Setor Público

Alcatel·Lucent
Enterprise

e-Book

Indice

Visão geral

Em todas as organizações do setor público, são os funcionários que realizam os negócios críticos do governo, nos quais todos confiamos. O papel deles não pode ser subestimado. Eles geralmente têm um impacto direto na vida de milhões de pessoas.

A digitalização está em andamento há algum tempo. Com a pressão contínua para melhorar os serviços públicos e cortar custos, a pandemia acelerou ainda mais essa tendência. Entretanto, não havia como o mundo ter previsto, há dois anos, a grande porcentagem de trabalhadores do setor público que passariam a trabalhar em casa, e o surgimento de uma força de trabalho distribuída.

Os desafios dos trabalhadores que esperam um mundo mais digital e os complexos requisitos de suporte a uma força de trabalho distribuída criaram a necessidade de as organizações do setor público migrarem de soluções temporárias para soluções mais permanentes, para apoiar a nova força de trabalho híbrida.

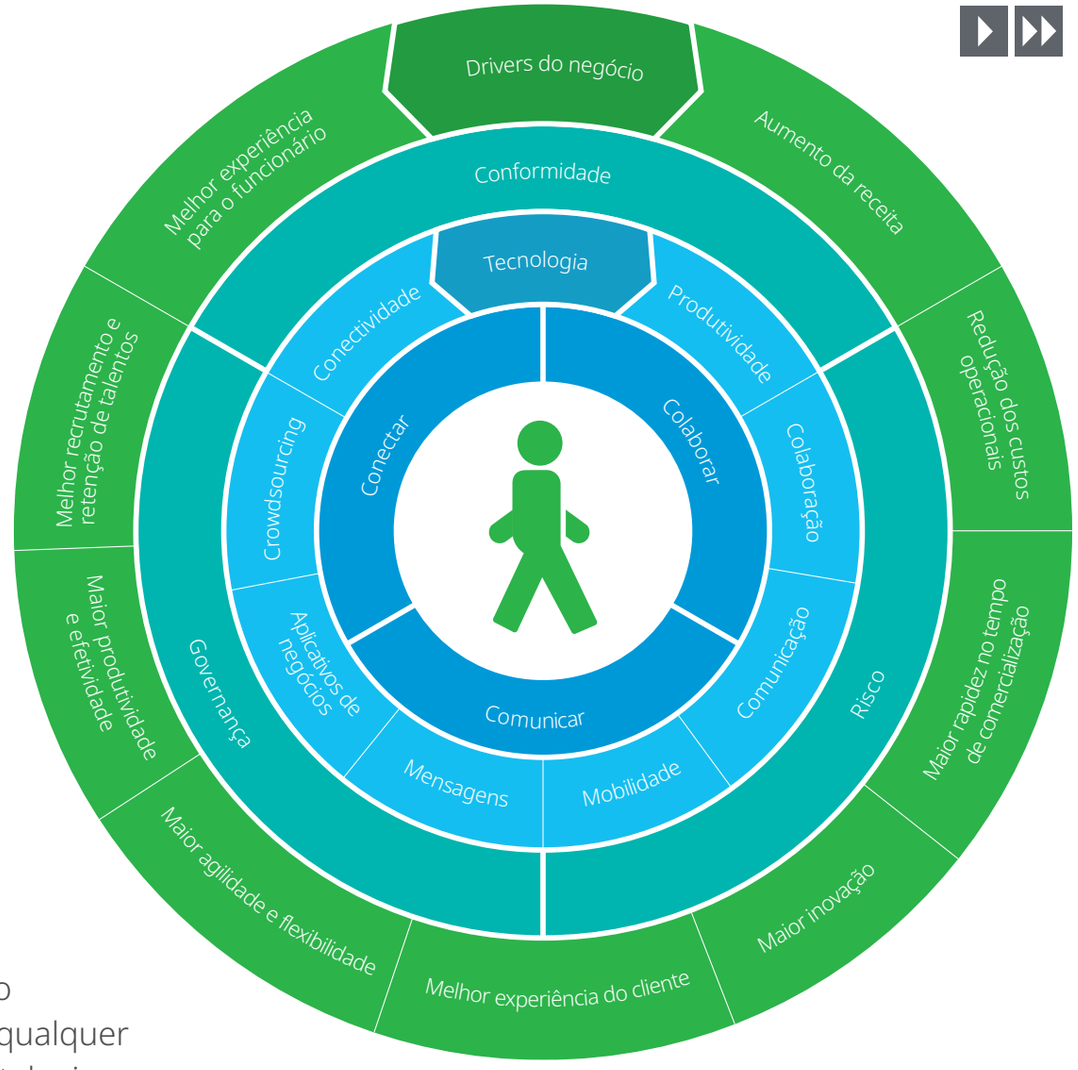
A Deloitte [1] fornece um excelente gráfico que explica como o ambiente de trabalho digital se encaixa, e as vantagens que ele oferece.

A tecnologia fornece ferramentas para melhorar as comunicações e a colaboração em qualquer local ou dispositivo. No entanto, garantir que você tenha a tecnologia certa para o resultado desejado pode ser mais complicado.

A Alcatel-Lucent Enterprise tem trabalhado com clientes em todo o mundo para entender os novos desafios que enfrentam e fornecer soluções de tecnologia digital que permitem que as forças de trabalho trabalhem de qualquer lugar, com qualquer dispositivo. O local de trabalho digital criou eficiências para os trabalhadores do setor público, permitindo maior produtividade com menos viagens, o que é um bônus para o planeta.

Este e-Book se concentrará nos três elementos-chave do local de trabalho digital para o setor público:

- Comunicação e colaboração
- Conectividade
- Segurança



E analisaremos as soluções ALE que podem ajudar as organizações do setor público a avançar com êxito em direção ao ambiente de trabalho digital com flexibilidade, agilidade e segurança.

1 - https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Principais considerações para o ambiente de trabalho digital do Setor Público

Comunicação e colaboração

Hoje, os funcionários dividem seu local de trabalho entre casa, locais remotos e o escritório. O escritório não é mais o local onde o trabalho acontece diariamente. É usado com mais frequência para reuniões de grupo, treinamentos e reuniões presenciais com os cidadãos. Os funcionários não vão mais a um único local para trabalhar e se reunir com suas equipes. Isso teve um impacto fundamental no ambiente de trabalho, tornando as comunicações e a colaboração mais importantes do que nunca.

As comunicações são um componente crítico para o sucesso do local de trabalho digital. Manter os funcionários engajados, produtivos e motivados é o desafio. Os funcionários precisam de ferramentas de comunicação que possibilitem suas atividades diárias e permitam que eles se comuniquem e colaborem com colegas, equipes e cidadãos, independentemente do local de trabalho ou de qualquer dispositivo.

Para garantir comunicações conectadas, recomendamos:

- Funções de comunicação avançada para funcionários, incluindo; voz de alta qualidade, chat em grupo, mensagens de voz e a capacidade de passar de uma chamada para um vídeo, independentemente do dispositivo
- Funções de colaboração, como compartilhamento de tela, controle remoto da área de trabalho e compartilhamento de arquivos grandes
- Comunicações seguras e colaboração com contatos externos
- Continuidade de chamadas em toda a organização com conexão instantânea e um diretório de contatos consistente
- Um canal de transmissão de notícias, mantendo todos atualizados sobre os últimos anúncios ou regulamentos
- As comunicações e a colaboração devem ser intuitivas

Para garantir que os funcionários tenham tudo o que precisam, recomendamos:

- Avaliar perfis de usuários e requisitos de comunicação, com base nas atividades dos funcionários, mobilidade e necessidade de acessar os aplicativos de negócios
- Oferecer aos funcionários da linha de frente dispositivos otimizados que permitem acesso rápido a informações e comunicações, mesmo quando em movimento

- Garantir que a equipe de atendimento ao cidadão tenha acesso otimizado ao gerenciamento de chamadas e interações, integrado ao CRM ou aos aplicativos de negócios
- Permitir colaboração com a equipe de backoffice para melhorar os serviços de atendimento ao cidadão e a resolução logo na primeira chamada
- Avaliar os requisitos legais locais/nacionais para proteger a privacidade dos dados

Para garantir um trabalho de alto desempenho em casa, recomendamos:

- Chat em grupo e reunião de áudio e vídeo com compartilhamento de tela para colaborar em qualquer dispositivo
- Continuidade de chamadas usando uma infraestrutura subjacente para conectar todos os perfis
- Uma opção DeskPhone para funcionários que passam mais de uma hora ao telefone e gerenciam chamadas importantes, como: atendimento ao cidadão, saúde e situações de emergência
- Comunicações dentro do aplicativo comercial preferido para facilitar a adoção pelo usuário e manter a área de trabalho organizada
- Acesso remoto seguro para acessar informações confidenciais com segurança

Conectividade

O local de trabalho digital depende de conectividade segura, resiliente e de alta qualidade. À medida que novas formas de trabalho se normalizam e o local de trabalho digital toma forma, a infraestrutura digital para conectar os funcionários deve estar pronta. Independentemente da localização, alguns pontos-chave devem ser levados em consideração.

- A segurança deve ser uma prioridade. É necessária uma solução de rede com várias camadas de segurança dentro da rede. Uma estrutura baseada em confiança zero pressupõe que cada dispositivo ou usuário é um risco de segurança. O controle de acesso à rede deve ser ativado.
- O acesso seguro a aplicativos, em qualquer lugar, cria a necessidade de conexões de acesso baseadas no usuário. Os perfis baseados no usuário fornecem conectividade segura e flexível sem perda de serviço, independentemente do local.
- Os funcionários remotos com altas exigências de segurança e privacidade de dados devem ser capazes de se conectar à rede corporativa a partir de casa ou das filiais. Isso assegura que as políticas corporativas e a segurança sejam mantidas, e a equipe de TI mantenha o controle.
- Os funcionários agora usam laptops para aplicações em tempo real (voz, vídeo) no escritório e em casa. Essa é uma grande mudança para muitas organizações do setor público. A rede sem fio deve ser capaz de suportar um maior uso de aplicativos em tempo real, em uma área maior. Isso deve ser considerado ao definir o escopo da rede.
- A resiliência da rede sem fio subiu na lista de prioridades, à medida que muito mais trabalhadores se conectam sem fio. Uma rede sem fio com inteligência distribuída nos pontos de acesso significa que não há um único ponto de falha e, no caso de um ponto de acesso ficar inativo, outros pontos de acesso da rede assumirão o serviço. Uma rede inteligente sem fio distribuída também elimina a necessidade de duplicação na rede, economizando tempo e dinheiro.
- O ritmo acelerado da transformação digital cria mais pressão para a equipe de TI, que já está lidando com tarefas do dia a dia. As eficiências que podem ser obtidas devem ser consideradas. Reduzir o número de interfaces de gerenciamento e sistemas operacionais na rede reduzirá as cargas de trabalho e o tempo de treinamento. Além disso, a automação reduzirá o tempo de implantação e gerenciamento de rede operacional.
- O acesso de alta qualidade é essencial. O local de trabalho digital cria eficiências para permitir maior produtividade. Se a conectividade for insuficiente, o aumento da produtividade será perdido.

Segurança

Segurança nas comunicações

Organizações governamentais e do setor público são alvos significativos para ataques cibernéticos. Utilizar o equipamento mais seguro disponível é essencial. As ferramentas integradas de gerenciamento devem permitir a supervisão de segurança em todos os elementos.

Além disso, os dispositivos móveis estão transformando o cenário das comunicações e aumentando a necessidade de segurança à medida que os invasores cibernéticos exploram os volumes crescentes de código contidos em todos os pontos de acesso. Criptografia de nível de defesa, privacidade de dados e ambientes de comunicação seguros exigem uma infraestrutura segura e disponível que seja eficiente e fácil de gerenciar.

Nossas recomendações:

Atualize e monitore seu sistema de comunicações:

- As atualizações do sistema são extremamente importantes em termos de segurança cibernética. Isso mantém seus sistemas de comunicação atualizados, com proteção contra as vulnerabilidade de software.
- Habilite o monitoramento do seu sistema de comunicações para rastrear atividades suspeitas, configurando limites de uso e alarmes no sistema de gerenciamento de rede

Autentique e criptografe:

- Possibilite a autenticação mútua entre todos os dispositivos (telefones e gateways) e o sistema de comunicação
- A sinalização deve ser criptografada para evitar ataques de envenenamento de protocolo e ataques to tipo 'man in-the-middle'
- As comunicações IP devem ser criptografadas para evitar escutas

Torne seus sistemas redundantes e adicione um componente de segurança:

- O risco nunca é igual a zero. Se um gateway ou o sistema de comunicação principal estiver inativo, um sistema de backup pode assumir o controle sem problemas quando houver redundância espacial.
- Adicione os componentes necessários para proteger seu sistema de comunicação, como um Session Border Controller ou um Reverse Proxy, enquanto os servidores de notificações são usados para alertar as pessoas necessárias

Eduque:

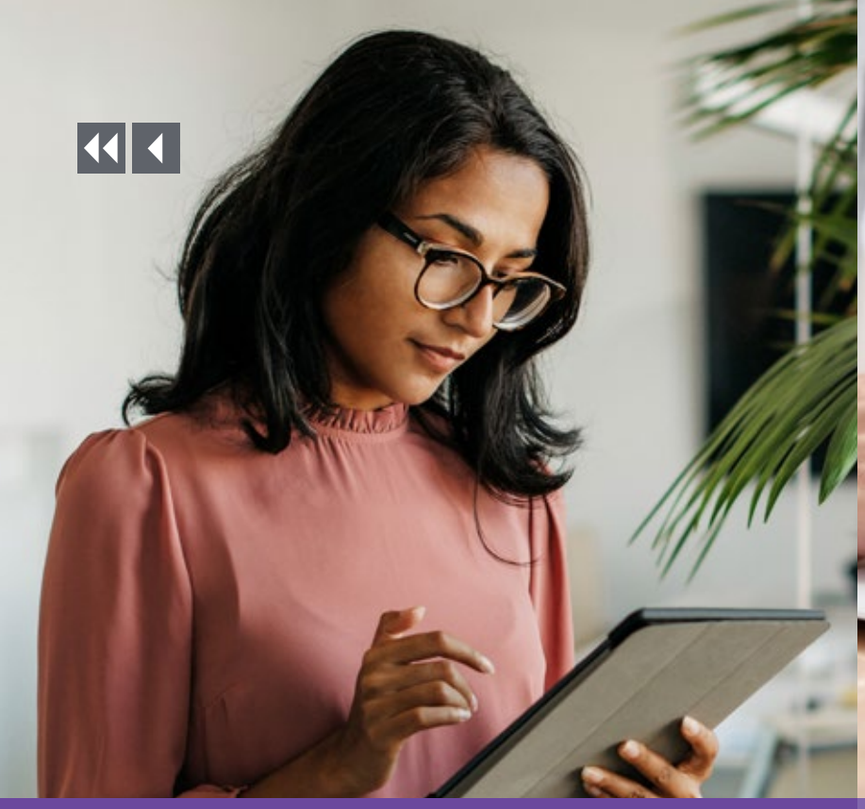
- Educar usuários e administradores; aplicar as melhores práticas dentro de suas equipes, incluindo lembretes para atualização de senhas, treinamento de usuários sobre como combater o crime cibernético e como reconhecer uma chamada codificada com o ícone do cadeado no telefone

Segurança de rede

A segurança cibernética ou cibersegurança é, há muito tempo, uma prioridade para as organizações governamentais. No entanto, as exigências de segurança cibernética estão mudando devido à transformação digital. À medida que a transformação se acelera, os velhos métodos de segurança de rede estão se tornando obsoletos. Como um componente fundamental da arquitetura de rede, a segurança deve ser integrada desde o início e aplicada universalmente em todos os acessos à rede — com e sem fio. A seguir estão algumas áreas a serem consideradas para proteger sua rede em todos os níveis.

- **Nível do usuário:** Verifique se os usuários estão sempre autenticados e autorizados com os direitos de acesso corretos (usando políticas e perfis)
- **Nível do dispositivo:** Verifique se os dispositivos são autenticados e estão em conformidade com as regras de segurança de TI estabelecidas. Isso pode ser feito com agentes instalados nos dispositivos, que executam uma verificação de segurança rápida antes que os dispositivos se conectem à rede. Por exemplo: a verificação pode garantir que os dispositivos que ingressam na rede tenham software antivírus atualizado e a versão mais recente do sistema operacional.
- **Nível de aplicação:** Defina regras associadas a aplicações específicas (incluindo bloqueio, limitação de largura de banda ou identificação de quem pode utilizá-las)
- **Análise inteligente:** As capacidades analíticas dos switches e access points ajudam a fornecer visibilidade e informações detalhadas sobre a rede, usuários, dispositivos, e aplicativos sendo utilizadas na rede. Eles também podem fornecer recursos de inspeção profunda de pacotes, que detectam o tipo de dados e aplicativos que se movem pela rede, tornando possível identificar padrões de tráfego de rede incomuns e atividades não autorizadas e intrusões na rede.
- **Técnicas de segmentação de rede:** colocar os dispositivos IoT em contêineres virtuais seguros permite que vários dispositivos e redes usem a mesma infraestrutura física, e ainda assim permaneçam isolados do restante da rede. Se ocorrer uma violação em uma parte da rede virtual, ela não afeta outras áreas da rede ou aplicações.

Essas técnicas de segurança ajudam a construir uma Arquitetura de Confiança Zero, o próximo nível em arquitetura de rede que opera a partir da premissa 'Nunca confie – Sempre verifique', onde todos os usuários devem ser autenticados, autorizados e continuamente validados antes de ter acesso aos dados e aplicativos.



Local de trabalho digital

Modelos flexíveis na nuvem

Conecte tudo

Soluções ALE para o ambiente de trabalho digital do Setor Público

Comunicação e colaboração

As Comunicações da Era Digital (DAC), da Alcatel-Lucent Enterprise, fornecem soluções de comunicação e colaboração abrangentes, locais ou baseadas na nuvem, para enfrentar a transformação digital. O local de trabalho digital está evoluindo para um ambiente de trabalho distribuído, onde o trabalho remoto se tornou normal, tornando as comunicações em tempo real essenciais para conectar colegas, cidadãos e parceiros. As soluções de comunicação da Alcatel-Lucent Enterprise permitem a continuidade de chamadas de qualquer lugar, em qualquer situação e de qualquer dispositivo.

Principais recursos de comunicação da ALE:

- **Conexão ininterrupta** dentro e fora da organização. A infraestrutura de comunicação subjacente conecta funcionários híbridos aos funcionários de back-office e da linha de frente, qualquer que seja seu dispositivo, por meio de uma variedade de tecnologias padrão como PSTN, TDM, IP, SIP, VoWIFI, DECT e também fornece métricas para que a TI monitore a Qualidade de Serviço (QoS).
- **O roteamento a um único número telefônico**, entre o telefone comercial e o softphone, é perfeito para o trabalho híbrido. Quer os funcionários estejam trabalhando em casa ou no escritório, nenhuma chamada é perdida e o encaminhamento de chamada não é necessário.

- Os DeskPhones da ALE são robustos, com **qualidade 3D Symphonic HD** e aplicativos de smartphone para a equipe móvel da linha de frente, incluindo notificações e alarmes em roaming no local
- **Fácil acesso** para atendimento aos clientes e recursos para os agentes, como grupos de chamadas e filas de espera, permitem que a equipe de atendimento ao cliente atenda a todas as chamadas
- **Uma Conferência de Crise por chamada de emergência** permite que contatos predefinidos sejam automaticamente inseridos em uma conferência para gerenciamento de desastres ou crises, apenas com o pressionar de um botão
- **A criptografia de ponta a ponta** fornece a garantia de segurança e privacidade necessária para organizações do setor público
- A comunicação e colaboração para o local de trabalho digital é fácil, com um simples **clique-para-ligar** para um contato ou iniciar uma conferência, ou recursos mais avançados, como chat em grupo, compartilhamento de tela e arquivos, reuniões de áudio e vídeo, tudo em um único aplicativo, disponível como um cliente web. Não é necessária nenhuma instalação. Os aplicativos estão disponíveis para dispositivos Android e iOS, bem como para PCs. Clientes com soluções ALE podem usar aparelhos já existentes com tecnologia WebRTC.
- Conectores para Microsoft® Teams e Google permitem que os funcionários **se comuniquem facilmente** com toda a organização, a partir de seu local de trabalho digital. Com os conectores Rainbow para SaaS CRM e ITSM, os funcionários se comunicam e colaboram a partir de seus aplicativos de negócios.

e-Book
Considerações e soluções para o ambiente de trabalho digital do Setor Público

Conectividade

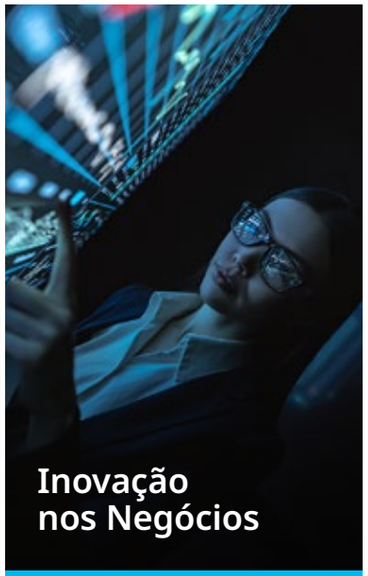
Digital Age Networking, da Alcatel-Lucent Enterprise, fornece uma rede autônoma que oferece uma experiência de conexão resiliente e contínua com o Alcatel-Lucent OmniSwitch® (LAN) e o Alcatel-Lucent OmniAccess® Stellar (WLAN) com tempo de convergência ultrarrápido, controle de acesso para rede segura e QoS garantido. O Wi-Fi corporativo de nova geração, com controle WLAN integrado nos pontos de acesso, elimina a necessidade de controladores físicos centralizados. As soluções ALE podem ser administradas localmente ou a partir da nuvem.

Principais características da conectividade ALE:

- **Um único Sistema de Gerenciamento de Rede (NMS)** fornece um nível adicional de integração entre redes com e sem fio, e reduz a carga de trabalho do gerente de TI pois não há necessidade de lidar com dois sistemas de gerenciamento, com dois conjuntos de políticas e regras de configuração. O Alcatel-Lucent OmniVista® Network Management System fornece gerenciamento unificado e visibilidade de toda a rede, ajudando a melhorar a eficiência e agilidade de TI.
- **O provisionamento automatizado** de uma infraestrutura de rede segura simplifica adições, movimentações e alterações, reduzindo o tempo necessário para manter e operar a rede, criando eficiência operacional e reduzindo custos e riscos.
- **Shortest Path Bridging (SPB)** projetado para suportar a criação e operação de uma rede menos complexa, constrói e mantém dinamicamente a tipologia de rede entre os nós. O SPB carrega e usa todas as conexões físicas disponíveis, disponibilizando mais largura de banda.
- **Funcionários híbridos (opção 1). O acesso remoto seguro** é habilitado com o Remote Access Point (RAP). A rede corporativa pode ser facilmente estendida para fora do local principal, fornecendo conectividade aos funcionários remotos como se estivessem na LAN da empresa. Dependendo do modelo, o RAP também pode fornecer conectividade com fio para telefones IP ou para outros dispositivos IoT. O acesso é suportado por políticas de segurança centralizadas e unificadas em redes com e sem fio, garantindo fácil gerenciamento e segurança altamente robusta e consistente.
- **Funcionários híbridos (opção 2) SD-WAN e SASE**. O Secure Access Service Edge (SASE) conecta de forma segura os locais remotos, filiais e funcionários remotos.A solução SASE para funcionários remotos consiste em um software no laptop do usuário que fornece acesso seguro a aplicações no data center da empresa, em data centers privados ou na Internet ou em nuvens públicas, com gerenciamento centralizado e sem a necessidade de hardware adicional para o funcionário. O SASE fornece segurança avançada com Firewall de Próxima Geração (NGFW), incluindo filtragem de URL e firewall de aplicativo, e Unified Threat Management (UTM), incluindo o Next Generation Intrusion Prevention System (NGIPS), antivírus e funcionalidade antimalware.

Automatizar as operações das redes de missão crítica e melhorar a experiência do usuário

Aumentar a digitalização, com a inclusão e gerenciamento seguro de IoT



Acelerar a transformação com fluxos de trabalho automatizados

Segurança

Segurança nas comunicações

Se você é responsável por um órgão governamental local, de pequeno ou grande porte, sua rede de comunicações corre o risco de ser alvo de hackers.

Principais recursos de segurança da ALE:

- **Conectividade segura** entre o sistema de comunicação local (PABX e telefones) e a infraestrutura de nuvem, totalmente desenvolvida e operada pela Alcatel-Lucent Enterprise, com autenticação mútua, criptografia e elementos de borda de segurança (SBC).
- **Alta disponibilidade** com arquiteturas espacialmente redundantes, nas instalações, em nuvens privadas ou públicas, proteção contra ataques de negação de serviço (DoS), segurança integrada com hardware robusto e sistemas operacionais.
- **Confidencialidade das comunicações** com criptografia sólida baseada em padrões industriais implementados nativamente na solução, sem qualquer impacto na qualidade e desempenho da voz, proporcionando a experiência que clientes e funcionários esperam.
- **Privacidade e proteção de dados** com controle de acesso baseado em funções e criptografia de dados armazenados. Isso assegura que todos os dados cruciais coletados no ambiente comercial em evolução estejam totalmente protegidos de ponta a ponta e sob seu controle.
- **Conformidade com regulamentos e normas** como (mas não se limitando a) Regulamento Geral de Proteção de Dados (GDPR), ISO27001, Critérios Comuns EAL2+, HDS (certificação de serviços em nuvem 'Hébergeur Données Santé' da ALE para conformidade de proteção de dados de pacientes na França).
- **Segurança como processo**, com Equipe de Resposta a Incidentes de Segurança de Produto (PSIRT) para gerenciamento ativo de vulnerabilidades, software atualizado regularmente e plataforma de políticas

ANSSI (CSPN)

ENS (Esquema Nacional de Seguridad)

Certificação estabelecida pelo Sistema Nacional de Segurança Espanhol a fim de ter um sistema que garanta a proteção adequada dos sistemas de informação contra ameaças e incidentes externos.

ISO27001 - 017/018

A Agência para uma Itália Digital está sob a Presidência do Conselho de Ministros. Ela regula o uso, armazenamento e acesso aos dados-chave, garantindo a segurança.

CERTIFICAÇÕES EM ANDAMENTO

Certificação BSI

Escritório Federal de Segurança da Tecnologia da Informação (Bundesamt für Sicherheit in der Informationstechnik). Equivelante ao CSPN da ANSSI (Q3 2021)

e-Book

Considerações e soluções para o ambiente de trabalho digital do Setor Público

Segurança de rede

A transformação digital mudou profundamente os requisitos de segurança cibernética. À medida que o número de dispositivos conectados aumenta, o perímetro da rede desaparece e as mudanças continuam a acelerar. A Digital Age Networking, da Alcatel-Lucent Enterprise, mantém seus ativos de TI e dados seguros na era da transformação digital atual. Com esta solução, você pode gerenciar de perto o acesso do usuário, reduzir as vulnerabilidades criadas pela IoT, dispositivos móveis e de rede, impedir que qualquer violação inevitável represente um ponto de ataque, e fornecer um ecossistema empresarial confiável.

As soluções ALE são projetadas para segurança, com:

- **Código Diversificado Seguro** que promove segurança e garantia no nível do dispositivo de rede, usando verificação e validação independente de terceiros, incluindo:
  - Análise de código-fonte, teste de 'black box / white box' por uma empresa especializada em segurança cibernética para eliminar vulnerabilidades, incluindo:
    - ¬ Ameaças de backdoor
    - ¬ Malware incorporado
    - ¬ Vulnerabilidades exploráveis
    - ¬ Exposição de informações proprietárias e/ou sigilosas
- **Diversificação de software:** o software ALE implementa a Randomização de Layout do Espaço de Endereço (ASLR). Cada inicialização de switch gera dinamicamente um layout de memória exclusivo para impedir ou prevenir a exploração de software.
- **Segurança de confiança zero (micro e macrossegmentação):** a estrutura baseada em confiança zero pressupõe a presença de hackers. A empresa não é mais considerada uma zona de confiança implícita. Isso envolve ações como autenticar todas as conexões. Nenhum ativo e nenhum usuário é inerentemente confiável.
- **Segurança por padrão:** o acesso remoto no OmniSwitch deve estar ativado, o que é o oposto da maioria dos outros switches, onde todos os acessos aos switches/roteadores são ativados por padrão e os administradores precisam descobrir como proteger o dispositivo.
- **Proteção integrada para Negação de Serviço (DoS):** proteção do sistema operacional e do módulo de gerenciamento contra uma série de ataques DDOS que normalmente são usados para fazer com que a CPU seja 100% utilizada.
- **Nenhum pacote de software** adicional: todos os recursos e capacidades, até mesmo o código de segurança ALE, estão incluídos no preço do switch — sem módulos para adicionar, sem atualizações para comprar. Todo o software está incluído.
- **Integração automatizada e segura de IoT:** por meio de impressão digital, classificação e conteinerização de dispositivos.

RGPD DA UE

Federal EUA

Interoperabilidade Conjunta dos EUA

Certificação MIL-STD dos EUA

Acordos Comerciais dos EUA Lei (TAA)

Saiba mais

Saiba mais sobre as soluções Alcatel-Lucent Enterprise para o Setor Público para o local de trabalho digital ou entre em contato conosco pelo site www.al-enterprise.com/pt-br/industries/government para conversar sobre as suas necessidades.

Alcatel·Lucent Enterprise