



CHECKLIST DE SEGURANÇA

Sua empresa está pronta para ataques feitos por IA?

40 verificações práticas, com as ferramentas que a Winit usa e indica.



POR QUE AGORA

Os ataques ficaram mais rápidos, automáticos e baratos

Agentes de IA tentaram invadir o site de um órgão público canadense, segundo pesquisadores. Eles agem com autonomia e se adaptam em tempo real: não seguem um roteiro fixo como um vírus tradicional.

Um grupo de ransomware com agentes de IA atacou ambientes Azure do início ao fim. Em sete minutos, apagou mais de 100 contas de armazenamento e removeu as proteções de backup. A porta de entrada conhecida: uma credencial vazada num repositório público.

Agentes de IA fizeram mais de 16 mil varreduras no site de uma agência da ONU, segundo a imprensa internacional. Qualquer empresa conectada à internet pode ser alvo.

A consequência prática: senhas curtas, MFA desligado, backup sem proteção e falta de monitoramento deixam de ser descuido pequeno e viram a porta aberta. Marque abaixo o que a sua empresa já cumpre.

Como usar: no Word, clique na caixinha para marcar. Cada item indica a ferramenta ou o serviço Winit relacionado, para você ver por onde começar.



Senhas e acessos

Quem entra, com o quê e até onde pode ir

01

- ☐ **Frases-senha longas e únicas.** Mínimo de 14 a 16 caracteres, uma para cada sistema. Nada de uma palavra só, nome + ano ou sequência de teclado: ferramentas automatizadas testam isso em instantes. [ORIENTAÇÃO DO TIME](#)
- ☐ **MFA ligado para todos os usuários.** Comece por administradores, financeiro e diretoria; prefira aplicativo autenticador ou chave de segurança ao SMS. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#) · [ENTRA ID](#)
- ☐ **Gerenciador de senhas corporativo** no lugar de planilha, post-it e senha salva no navegador. [A WINIT AJUDA A ESCOLHER E IMPLANTAR](#)
- ☐ **Administrador só para quem precisa.** Contas de admin separadas das contas do dia a dia e com o menor privilégio possível. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#) · [RBAC](#)
- ☐ **Quem sai, perde o acesso no mesmo dia.** E-mail, VPN, sistemas e licenças revogados; contas ativas revisadas a cada trimestre. [GLPI](#) · [INVENTÁRIO TI](#)



Computadores e celulares

Cada dispositivo protegido, atualizado e visível

02

- ☐ **Proteção de endpoint única e padronizada**, com console central. Antivírus diferente em cada máquina vira ponto cego. [ESET PROTECT](#)
- ☐ **Celulares e tablets gerenciados (MDM).** Senha de tela obrigatória e apagamento remoto em caso de perda ou roubo. [ESET PROTECT](#) · [MDM](#)
- ☐ **Atualizações automáticas** de Windows, Office, navegadores e firmware, com relatório do que está pendente. [DATTO RMM](#) · [KASEYA](#)

- ☐ **Disco criptografado nos notebooks** (ex.: BitLocker): perder o equipamento não pode virar vazamento. [RMM](#) · [POLÍTICA DE TI](#)
- ☐ **Inventário vivo de máquinas, softwares e licenças.** O que não se enxerga não se protege. [INVENTÁRIO TI](#) · [GLPI](#)



Rede e acesso remoto

O perímetro que separa a empresa da internet

03

- ☐ **Firewall com regras revisadas** e atualizado, administrado só pela rede interna. Senhas padrão de roteadores, câmeras e impressoras trocadas. [PFSENSE](#) · [OPNSENSE](#)
- ☐ **Rede segmentada.** Wi-Fi de visitantes, câmeras e equipamentos IoT separados da rede onde ficam os servidores e o financeiro. [VLANS NO FIREWALL](#)
- ☐ **Acesso remoto só por VPN com MFA.** Nenhuma porta de RDP ou SSH aberta direto para a internet. [PFSENSE](#) · [OPNSENSE](#)
- ☐ **Rede monitorada:** queda, pico de tráfego e dispositivo novo na rede geram alerta para alguém que responde. [ZABBIX](#) · [GRAFANA](#)
- ☐ **Filtro de navegação / proxy** para bloquear sites maliciosos e reduzir cliques perigosos. [FIREWALL](#) · [ESET](#)



Backup e recuperação

A última linha de defesa contra o ransomware

04

- ☐ **Regra 3-2-1:** três cópias, em duas mídias diferentes, uma delas fora do local (ou fora da nuvem principal). [DATTO BACKUP](#)
- ☐ **Cópia protegida contra exclusão.** Backup imutável ou offline e contas de backup separadas das contas de administração: ataques recentes apagam os backups primeiro. [DATTO](#) · [PROXMOX](#)
- ☐ **Teste de restauração agendado,** ao menos a cada trimestre, com o tempo medido. Backup que nunca foi restaurado é aposta. [ROTINA WINIT](#)
- ☐ **Metas por sistema crítico:** quanto de dado a empresa aceita perder (RPO) e quanto tempo suporta parada (RTO). [GOVERNANÇA WINIT](#)
- ☐ **Microsoft 365 também tem backup.** Lixeira e retenção padrão não são backup. [DATTO](#)



Monitoramento e resposta

Ver cedo e saber o que fazer na hora H

05

- ☐ **Alertas de login suspeito ativos:** horário ou país incomum, muitas tentativas, acesso de conta desligada. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#) · [WAZUH](#)
- ☐ **Logs centralizados** e guardados por tempo suficiente para investigar o que aconteceu. [WAZUH](#)
- ☐ **Alertas chegam a quem responde,** inclusive fora do horário, com quem aciona quem quando o primeiro não atende. [ZABBIX](#) · [RMM](#)
- ☐ **Plano de resposta de uma página:** quem decide, quem liga, como isolar a máquina e quando avisar clientes e a ANPD. [GOVERNANÇA WINIT](#)
- ☐ **Incidentes e chamados registrados** com histórico: o que aconteceu hoje vira prevenção amanhã. [GLPI](#) · [ZAMMAD](#)



E-mail e pessoas

Boa parte dos ataques começa numa mensagem

06

- ☐ **SPF, DKIM e DMARC configurados** no domínio, para que ninguém use o nome da empresa para enganar clientes. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#) · [DNS](#)
- ☐ **Filtro anti-phishing e anti-spam ativos**, com bloqueio de anexos executáveis. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#)
- ☐ **Treinamento curto e recorrente**. Conversas em pequenos grupos funcionam melhor que um manual que ninguém lê. [ENDOMARKETING DE SEGURANÇA](#)
- ☐ **Pedido urgente de pagamento ou troca de conta bancária** só com confirmação por um segundo canal conhecido. Voz e vídeo falsos feitos por IA já são realidade. [PROCEDIMENTO DO FINANCEIRO](#)
- ☐ **Canal fácil para avisar "cliquei errado"**, sem medo de punição: quanto antes se sabe, menor o estrago. [CULTURA DE SEGURANÇA](#)



IA com segurança na empresa

Usar a IA a favor, sem abrir porta

07

- ☐ **Política curta de uso de IA**: o que pode e o que nunca pode ser colado (senhas, dados pessoais, contratos, segredos do negócio). [IA NA ADMINISTRAÇÃO](#) · [WINIT](#)
- ☐ **Somente contas corporativas, com MFA**, em Claude, ChatGPT, Gemini e Grok. Conta pessoal não recebe dado da empresa. [CONTAS CORPORATIVAS](#)
- ☐ **Dado sensível fica em casa**: modelos abertos em servidor próprio para documentos e dados pessoais que não podem ir para a nuvem. [OLLAMA](#) · [OPEN WEBUI](#)
- ☐ **Agentes e automações com permissão mínima**, limite de gasto, registro de cada ação e aprovação humana para o que mexe com dinheiro ou dados. [POWER AUTOMATE](#) · [M365](#)
- ☐ **Chaves e segredos fora de repositórios e planilhas**, com varredura periódica: no ataque ao Azure, a porta foi uma credencial vazada em um repositório público. [REVISÃO DE SEGREDOS](#)



Nuvem, dados e LGPD

Onde estão os dados e quem responde por eles

08

- ☐ **Permissões do Microsoft 365 revisadas** (SharePoint, OneDrive, Teams): ninguém com acesso "a todos" sem necessidade. [ORIENTAÇÃO WINIT](#) · [MICROSOFT 365](#)
- ☐ **Em nuvem (Azure e similares)**: menor privilégio, recursos críticos com bloqueio contra exclusão e alerta para atividade anormal. [REVISÃO DE NUVEM](#)
- ☐ **Arquivos sensíveis em armazenamento com controle de acesso** e trilha de auditoria sob o seu comando. [NEXTCLOUD](#)
- ☐ **Mapa dos dados pessoais**: o que a empresa coleta, onde guarda, por quanto tempo e quem acessa. Política de privacidade em dia. [LGPD](#) · [WINIT](#)
- ☐ **Política de Segurança da Informação escrita**, aprovada pela diretoria e revisada ao menos uma vez por ano. [GOVERNANÇA WINIT](#)

QUANTOS VOCÊ MARCOU?

Leia o seu resultado

Até 20 itens

Prioridade alta. Há lacunas básicas que um ataque automatizado encontra rápido. Comece por MFA, backup protegido e atualizações.

21 a 32 itens

Bom caminho, mas falta consistência. Falta transformar o que existe em rotina: monitoramento, teste de backup e plano de resposta.

33 a 40 itens

Nível avançado. Mantenha revisões periódicas e treine o time: a ameaça muda mais rápido que as ferramentas.



Quantos itens a sua empresa cumpre de verdade?

Peça o diagnóstico gratuito de maturidade, segurança e conformidade e receba um relatório com as prioridades.

www.winit.com.br/avaliacao-gratuita · adm@winit.com.br · (51) 98016-3670 (RS) · (47) 99273-4515 (SC)

Checklist orientativo, não substitui diagnóstico técnico. A Winit atua como MSP (opera o ambiente) ou como revenda (licenças oficiais e suporte). Marcas de terceiros pertencem aos seus respectivos proprietários e são citadas apenas para identificar as soluções utilizadas e revendidas.