

MANUAL PARA QUEM ESTÁ A COMEÇAR

O MiniPC. A central. A sua equipa.

Como aceder, instalar, acompanhar
e proteger os computadores da Veloma.

[ACESSO REMOTO](#)[SEGURANÇA](#)[PACOTES](#)[SENHAS](#)

01 · COMECE POR AQUI

Para que criámos isto?

Para apoiar a equipa, reduzir deslocações e manter os computadores organizados.

EXEMPLO REAL DE UTILIZAÇÃO

“O computador da contabilidade deixou de imprimir.”

O colaborador pede ajuda. O suporte entra no computador autorizado, observa o problema, corrige e regista o resultado. A central permite fazer isso sem estar à mesma mesa.

01 / Resolver à distância

MeshCentral permite ver o ecrã, controlar o computador e transferir ficheiros depois de instalar o seu agente.

02 / Acompanhar a segurança

Wazuh reúne inventário e alertas dos equipamentos cadastrados. Não é, por si só, um antivírus.

03 / Verificar ficheiros

ClamAV analisa ficheiros na central. No Windows, o **Defender** continua a proteção local em tempo real.

04 / Padronizar o trabalho

O **hub de pacotes** organiza instaladores; o **WSUS** centraliza atualizações Windows. A imagem de instalação é uma etapa ainda pendente.

O MiniPC é a sala de ferramentas.

Cada computador precisa de preparação própria. Ligar o MiniPC não instala agentes, programas ou antivírus automaticamente nos outros equipamentos.

Escolha o que precisa

Abrir os painéis · pág. 5

Acesso remoto · pág. 7

Instalar agentes · págs. 8–9

Antivírus · pág. 10

Senhas expostas · pág. 13

Primeiro piloto · pág. 16

02 · O QUE JÁ EXISTE

Pronto não significa instalado em todos.

Use esta fotografia do projeto para saber o que pode exigir hoje.

Recurso	Estado verificado	O que falta para usar na equipa
Painel de suporte	Disponível Login e ligação web testados; temas dia/noite.	Cadastrar e validar um primeiro PC com agente MeshCentral.
Wazuh	2 agentes ativos Veloma-Infra e Veloma-WSUS.	Instalar agentes nos postos e validar a comunicação da loja com o gestor.
Antivírus central	Serviços ativos ClamAV, assinaturas e API.	Definir as pastas e a rotina de cada equipamento.
Cliente do Mac atual	Configurado Downloads e Desktop, a cada 6 horas.	É uma análise de pastas; não é proteção integral em tempo real.
Pacotes e perfil Windows	Publicados	Testar numa máquina piloto antes da distribuição em massa.
Imagem Windows / PXE	Ainda pendente	Criar, capturar e homologar a imagem e o arranque pela rede.
Cofre: auditoria de vazamentos	Proposta	O módulo de auditoria ainda não foi implantado nem executado.

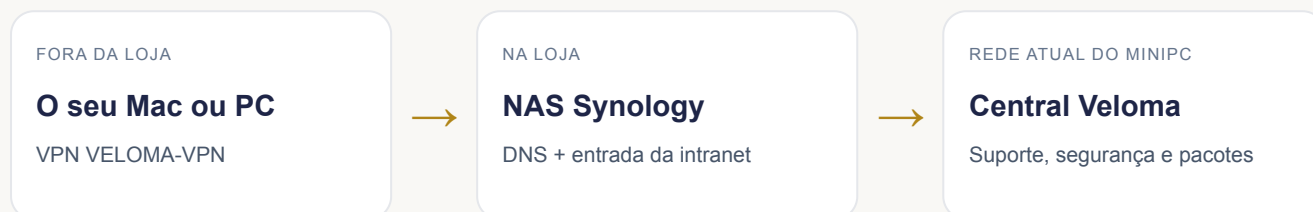
Não confunda descoberta com proteção.

Foram vistos 13 dispositivos na LAN atual do MiniPC. Essa rede é diferente da rede do NAS da loja. Esse número não é um inventário confirmado dos computadores da loja.

03 · ENTENDA A REDE

Como a ligação chega à Veloma.

A VPN é a passagem privada. O NAS é a porta de entrada. O MiniPC guarda as ferramentas.



O NAS e o MiniPC estão, hoje, em **redes físicas diferentes**. Existe uma ligação segura entre ambos. Usam faixas de IP parecidas; por isso, prefira os nomes da intranet a tentar adivinhar endereços numéricos.

Antes de abrir os painéis

- 1 Fora da loja: ligar a VPN.**
No Mac atual, abra Tunnelblick e ligue **VELOMA-VPN**. Aguarde o estado **Conectado**.
- 2 Confirmar o DNS.**
O DNS transforma nomes em endereços. Na VPN atual é distribuído pelo NAS. Na loja, a distribuição automática pelo DHCP do roteador ainda precisa de configuração; a TI pode preparar cada estação.
- 3 Confirmar o certificado.**
A intranet usa agora certificado público Let's Encrypt. O navegador atualizado deve reconhecê-lo sem importar uma CA privada. Se surgir aviso, confira VPN/DNS e a hora do dispositivo com a TI; não desative a proteção.

E os endereços 127.0.0.1?

Significam “este computador”. Os links com portas 19444/19443 funcionam no Mac onde o túnel foi instalado. Copiá-los para outro PC não cria acesso. Use os nomes da intranet quando a VPN e o DNS estiverem preparados.

04 · OS SEUS FAVORITOS

Que endereço devo abrir?

Guarde estes links no navegador. A rede/VPN e o DNS precisam de estar preparados; o HTTPS usa certificado público.

Quero...	Abrir	Serve para
Ajudar num computador	suporte.intra.veloma.app	Painel MeshCentral: ecrã, ficheiros e terminal.
Ver alertas e inventário	seguranca.intra.veloma.app	Wazuh: agentes, riscos e eventos.
Obter instaladores	pacotes.intra.veloma.app	Catálogo de pacotes da central.
Consultar a descoberta de rede	inventario.intra.veloma.app	Relatório técnico em JSON, não uma lista de PCs já protegidos.
Consultar backups	backup.intra.veloma.app	UrBackup; exige cliente e política de cópia configurados.
Consultar imagens	imagens.intra.veloma.app	Biblioteca de ficheiros de instalação.
Administrar o MiniPC	servidor.intra.veloma.app	Cockpit; reservado à equipa técnica.
Administrar o NAS	nas.intra.veloma.app	DSM Synology; credenciais do NAS são separadas.

Entrar sem confundir as contas

A conta **suporte** da central foi entregue ao responsável por canal privado. Este manual não contém senhas. O NAS, os computadores e o Veloma Connect podem ter contas diferentes.

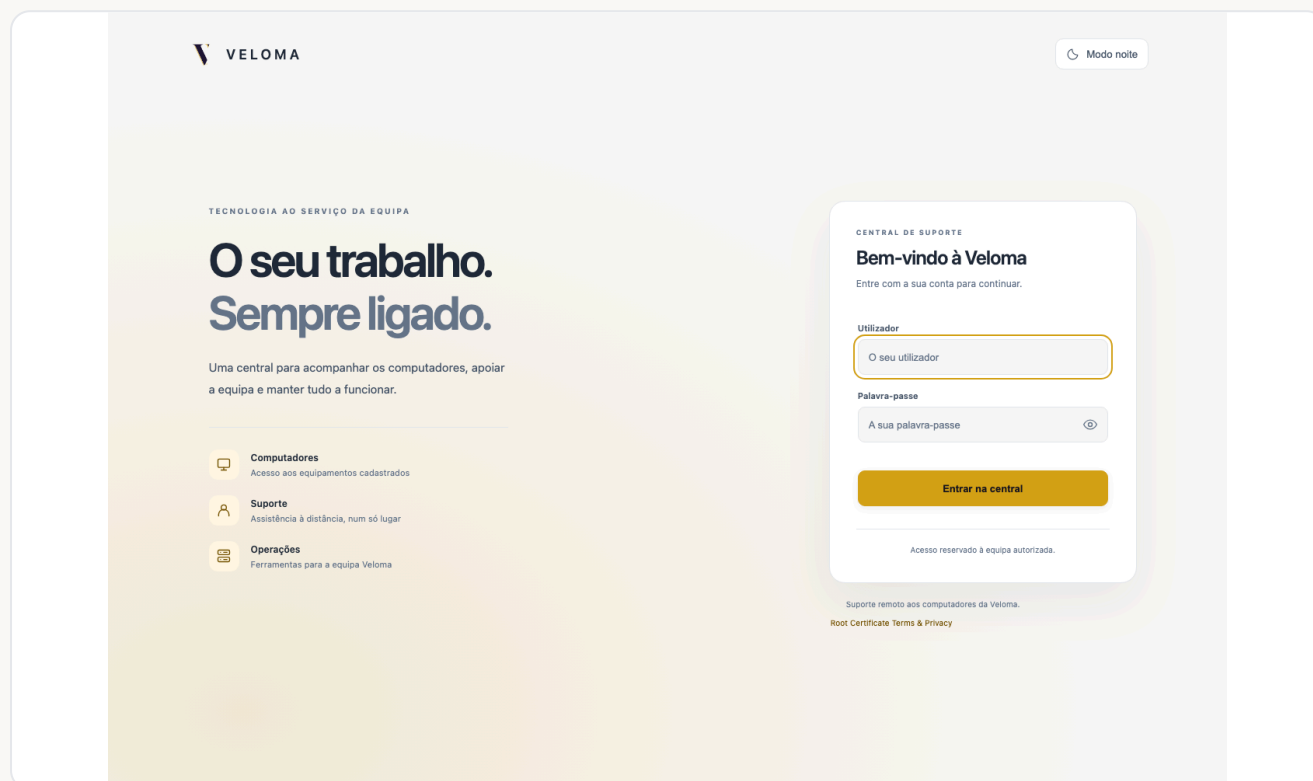
Duas aplicações, duas funções.

O Veloma Connect em vav.veloma.app é o atendimento/CRM. O painel MeshCentral é a ferramenta para controlar computadores. Uma senha redefinida no Connect não altera automaticamente os outros serviços.

05 · PRIMEIRO ACESSO

O painel de suporte, sem mistério.

Esta é uma captura real da interface criada para a Veloma.



Login real · modo dia. As senhas não foram incluídas na captura.

1. Escolha o tema

Modo dia / Modo noite, no topo. A preferência fica guardada nesse navegador.

2. Escreva o utilizador

Use a conta de suporte entregue pelo responsável. Depois introduza a palavra-passe.

3. Confira a senha

O ícone de olho mostra/oculta o texto. Use-o apenas quando ninguém estiver a observar o ecrã.

4. Entre na central

Clique em **Entrar na central**. Se o visual antigo persistir, no Mac use **⌘ + Shift + R**.

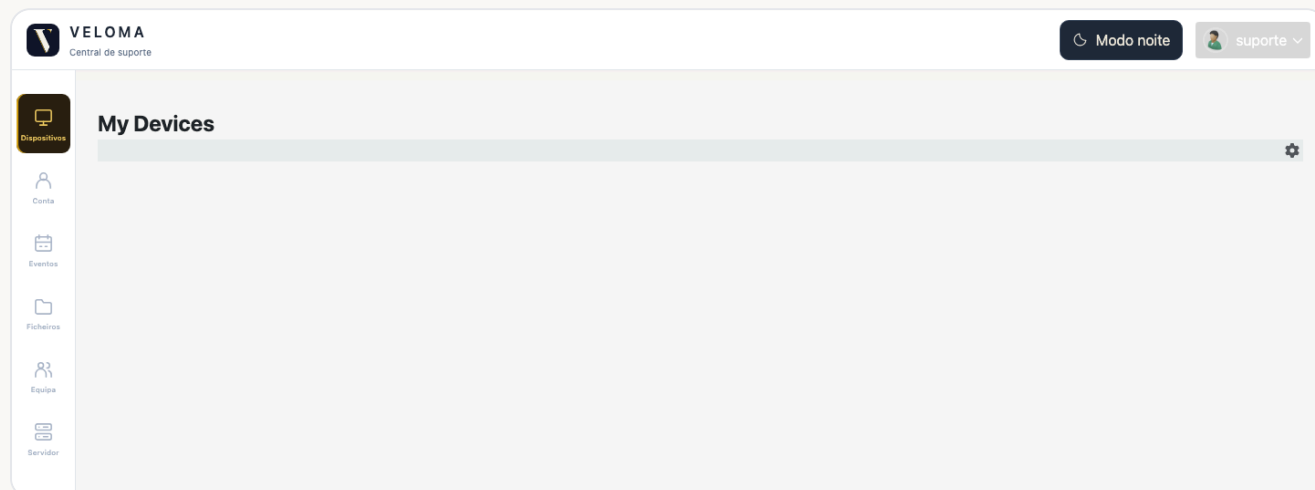
Se não entrar

Anote o endereço aberto e a mensagem exata. “Não resolve o nome” aponta para DNS/VPN; “senha inválida” é autenticação. Não repita dezenas de tentativas nem use a senha de outra aplicação.

06 · SUPORTE REMOTO

Como entro no computador de alguém?

Primeiro, esse computador precisa de aparecer no MeshCentral e estar ligado à rede.



Captura real da fase inicial: sem grupos ou PCs cadastrados nesse momento. Não é uma simulação de equipamentos protegidos.

- 1 **Abra Dispositivos.**
É o ícone do computador na barra lateral. Selecione o grupo da empresa e depois o equipamento correto, por exemplo **VELOMA-PC-001**.
- 2 **Confirme a pessoa e o pedido.**
Verifique o nome do colaborador. Avise que vai iniciar a assistência e confirme a autorização aplicável.
- 3 **Escolha o tipo de acesso.**
Desktop / Ambiente de trabalho: ver e controlar o ecrã. **Files / Ficheiros:** transferir ficheiros. **Terminal:** comandos técnicos; deixe essa opção para a TI.
- 4 **Termine e registe.**
Desligue a sessão de suporte e registe o que foi feito. Não mantenha documentos do colaborador abertos sem necessidade.

Offline não quer dizer avariado.

O PC pode estar desligado, suspenso, sem Internet ou sem agente. A central não liga fisicamente um equipamento que não tenha gestão de energia/remota preparada.

07 · INSTALAR NUM PC WINDOWS

O primeiro computador da equipa.

Procedimento do suporte, com privilégios administrativos. Comece por uma máquina piloto.

1 Preparar a identidade.

Registe o responsável e reserve um nome: **VELOMA-PC-001**, depois 002, 003... Confirme a edição Windows e guarde as credenciais num cofre.

2 Criar ou escolher o grupo.

No MeshCentral, o administrador cria um **Device group / Grupo de dispositivos** para os computadores Veloma. Dentro dele, escolha **Add agent / Adicionar agente**.

3 Obter o agente correto.

Selecione Windows e a arquitetura indicada. O instalador deve vir da própria central, já associado ao grupo. **Não descarregue um servidor MeshCentral novo para cada PC.**

4 Instalar no PC de destino.

Execute o instalador do agente como administrador e aceite o pedido legítimo do Windows. O agente fica como serviço e inicia com o sistema.

5 Confirmar o resultado.

Volte ao painel, atualize a lista e confirme o nome. Teste o ecrã e uma transferência de ficheiro de teste. Só depois repita nos outros PCs.

6 Adicionar a monitorização.

Instale também o **agente Wazuh** obtido no hub, cadastrado no gestor correto. Confirme o estado **Active / Ativo** no Wazuh. Mantenha o Defender ligado.

Passo de rede obrigatório antes da distribuição.

A ligação web por NAS já foi testada. A ligação de um novo agente da loja ainda exige piloto: a TI precisa confirmar o endereço gerado no instalador, a rota e o certificado. Os scripts Wazuh atuais usam 192.168.1.229 por omissão; esse endereço não identifica a mesma rede na loja. Não execute em massa sem corrigir e validar o destino.

08 · MAC E ALTERNATIVAS

No Mac, há permissões adicionais.

Instalar um agente não dá automaticamente autorização para ver ou controlar o ecrã.

1 Obter o agente do grupo correto.

No MeshCentral, escolha macOS e a arquitetura compatível: Apple Silicon ou Intel. Use o comando/instalador fornecido pela central e execute-o com a conta administrativa.

2 Autorizar o que o macOS pedir.

Em **Definições do Sistema** → **Privacidade e Segurança**, verifique as permissões de Acessibilidade e de gravação/controlo do ecrã para o agente. Os nomes variam com a versão. Não conceda acesso a aplicações desconhecidas.

3 Testar ver e controlar.

Se aparece imagem mas não consegue usar o rato, confira Acessibilidade. Se o ecrã fica preto, confira a permissão de captura/ecrã. Pode ser necessário reabrir o agente ou a sessão.

4 Adicionar Wazuh separadamente.

O Wazuh tem instalador próprio. O agente de sistema do Mac atual ainda depende da instalação administrativa; o cliente de análise de ficheiros já existente não substitui esse agente.

Ferramenta	Quando usar	O que é necessário
MeshCentral	Suporte centralizado pelo navegador.	Agente instalado, cadastro e ligação ao servidor.
RDP / Windows App	Entrar numa sessão Windows remota.	Windows compatível para receber RDP, conta permitida e rota pela LAN/VPN. Windows Home não recebe RDP nativamente.
AnyDesk	Alternativa de assistência remota.	Cliente instalado e política de acesso própria. Acesso não supervisionado e uso comercial exigem configuração/licenciamento adequados.

Instalar programas remotamente

Depois de obter acesso autorizado ao PC, a TI pode transferir e executar o instalador. RDP e MeshCentral não contornam a senha administrativa nem as permissões do sistema.

09 · ANTIVÍRUS

O que está a proteger o quê?

Há três camadas complementares, com funções diferentes.

NO WINDOWS

Defender

Proteção local em tempo real. Continua ativo mesmo que a central esteja inacessível. Não o desligue para “usar o antivírus do MiniPC”.

NA CENTRAL

ClamAV

Analisa os ficheiros recebidos pelo serviço e as pastas partilhadas configuradas. As assinaturas são atualizadas pelo serviço FreshClam.

NA MONITORIZAÇÃO

Wazuh

Reúne eventos e alertas de segurança dos agentes. Não significa que cada PC tenha um antivírus instalado ou todos os discos analisados.

No Mac já preparado

O cliente atual verifica **Downloads e Desktop a cada seis horas**, enquanto o Mac está ligado e consegue chegar à central pelo túnel. Envia o conteúdo dos ficheiros elegíveis por ligação protegida ao MiniPC; a API não os guarda como uploads.

A última execução observada analisou **812 ficheiros sem deteção** e deixou **6 por analisar**, por limites de tamanho/complexidade. Ficheiros já limpos podem ser reutilizados do histórico quando o ficheiro e as assinaturas não mudaram.

Limite real da solução.

Esse cliente não vigia todo o Mac em tempo real, não analisa automaticamente todas as pastas e não elimina nem põe ficheiros em quarentena. A API não é uma página web de upload. Uma varredura sob pedido precisa do cliente técnico ou de outra interface ainda a preparar.

10 · LER OS RESULTADOS

Quando devo agir?

Um alerta deve ajudar a decidir; não serve para declarar que todos os computadores estão seguros.

Resultado	Significado	Ação prática
clean Sem detecção	Não foi detetada ameaça no ficheiro efetivamente analisado.	Continuar a rotina. Não é uma garantia absoluta.
detected Detetado	O motor identificou uma assinatura ou ameaça.	Não abrir nem partilhar o ficheiro. Registrar o alerta e chamar o suporte para confirmar e tratar.
unscanned Não analisado	O limite de tamanho, conteúdo do arquivo ou alteração durante a leitura impediu a análise.	Pedir análise adicional à TI. Não classificar como limpo nem assumir que é infeção.
error Erro	Houve uma falha de acesso, rede ou processamento.	Verificar a ligação e repetir a análise depois da correção.

Onde consulto?

No **Wazuh**, selecione o agente e procure os alertas relacionados com antivírus. Apenas eventos efetivamente recebidos aparecem ali. Os nomes dos menus variam com a versão.

No Windows, consulte também **Segurança do Windows** → **Proteção contra vírus e ameaças** → **Histórico de proteção**. No Mac atual, o detalhe da última análise está no relatório local, que o suporte pode ler.

Se suspeitar de infeção

Pare de abrir o ficheiro, anote o nome do PC, a hora e a mensagem. Se houver encriptação de ficheiros ou atividade claramente maliciosa, desligue a rede desse PC e contacte imediatamente a TI. Não apague evidências nem “limpe tudo” sem diagnóstico.

11 · INSTALAÇÕES E ATUALIZAÇÕES

Como preparo um PC de trabalho?

A central reúne materiais. A instalação continua a precisar de uma máquina alvo, autorização e validação.

1 Usar o hub de pacotes.

Abra **pacotes.intra.veloma.app**. Em **windows/workstation/** estão o perfil, os recursos visuais e **DEPLOYMENT.txt**; o pacote é **windows/veloma-workstation-v1.zip**. A TI valida a origem e o checksum do catálogo.

2 Aplicar o padrão Veloma.

O perfil prepara **adminveloma** para administração e **colaborador** para o trabalho diário, nome do responsável, identidade visual, RDP na LAN/VPN, AnyDesk e 7-Zip. Use credenciais individuais no posto.

3 Ativar os produtos licenciados.

O Microsoft 365 Family precisa de instalação e ativação pela conta com direito de uso. O pacote não contém contas Microsoft nem ativações clonadas.

4 Atualizar antes de entregar.

O WSUS tem grupos **Piloto** e **Producao**, sincronização diária e aprovação manual. Os PCs precisam de política de cliente e comunicação válida; verificação final é no Windows Update do próprio PC.

Ainda não existe uma imagem Veloma pronta para apagar e instalar PCs.

A imagem Windows personalizada, captura generalizada, arranque PXE e instalação completa em piloto ainda precisam de ser construídos e homologados. O pacote publicado é uma preparação pós-instalação, não uma ISO/WIM final.

A licença também faz parte da entrega.

A VM WSUS usa Windows Server de avaliação. A licença de produção está pendente. Não há KMS público configurado. Um PC só deve ser entregue depois de validar licença, agentes e aplicações.

12 · SENHAS EXPOSTAS

Podemos analisar o nosso cofre?

Sim. Podemos procurar sinais concretos de risco sem publicar as senhas completas.

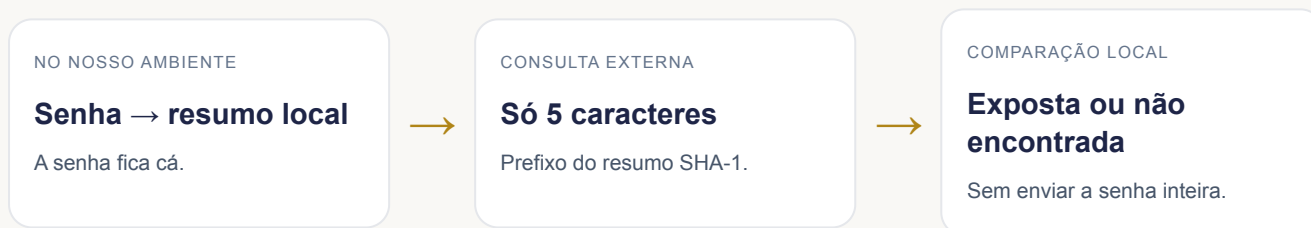
O que conseguimos detetar

Senhas repetidas entre serviços; combinações fracas; credenciais sem revisão; e correspondência com senhas presentes em bases públicas de vazamentos.

O que isso não prova

Uma correspondência não identifica automaticamente a conta afetada, o site onde a Veloma usou a senha, nem prova que alguém entrou nessa conta.

Verificação por prefixo, explicada de forma simples



O serviço Pwned Passwords permite esse método. A consulta informa se a mesma combinação está no conjunto conhecido. SHA-1 aqui é usado como identificador de consulta; não é a forma recomendada para guardar senhas de utilizadores.

“Não encontrada” não é “segura”.

A base não conhece todos os incidentes. Uma senha pode ser reutilizada, previsível ou ter sido roubada recentemente e ainda não aparecer. Por isso, a avaliação junta vazamento conhecido, reutilização e política de acesso.

Importante sobre esta entrega

Nenhuma senha do cofre foi consultada numa base de vazamentos para produzir este manual. A auditoria é uma função proposta, ainda não um serviço ativo da central.

13 · AUDITORIA DO COFRE

Como seria o relatório da Veloma?

O resultado deve orientar a correção e identificar o responsável, sem mostrar a senha.

Se o cofre for o **Veloma Acessos**, os dados estão cifrados com uma chave derivada da senha mestra. O auditor precisa de uma sessão autorizada e desbloqueada. Se for o **Chaves do macOS**, o acesso depende das permissões desse cofre. Não existe um desbloqueio universal.

1 Ler no ambiente autorizado.

Analisar apenas os registos da organização a que o responsável tem acesso. Evitar exportações de texto simples e eliminar qualquer temporário de forma controlada.

2 Comparar e classificar.

Identificar reutilizações localmente e consultar a presença em vazamentos pelo método de prefixo. Não registar senhas nem hashes completos no relatório.

3 Gerar uma lista de ações.

Mostrar serviço, utilizador mascarado, risco e ação. Relatar erro de consulta como **não verificado**; nunca como “sem risco”.

4 Corrigir com o dono do serviço.

Trocar senhas expostas e reutilizadas, encerrar sessões suspeitas e ativar MFA onde disponível. Validar que os robôs e integrações continuam a funcionar após a rotação.

Exemplo ilustrativo	Resultado	Ação
Correio · c***@empresa	Presente na base conhecida + reutilizada	Trocar em todos os serviços onde era repetida.
ERP · f***@empresa	Não encontrada, mas repetida	Criar senha exclusiva e rever MFA.
Portal · a***@empresa	Consulta falhou	Manter como não verificada e repetir.

E descobrir em que site a senha foi usada?

O cofre indica onde guardámos uma credencial. Registos de login do serviço podem mostrar utilização real. Consultas de vazamentos de e-mail são outra função, com condições próprias e eventual subscrição. Uma pesquisa de senha, isolada, não liga uma senha a um e-mail, a um site ou a um invasor.

14 · ROTINA DA EQUIPA

Como isto entra no dia a dia?

Uma rotina curta é mais útil do que abrir todos os painéis sem saber o que procurar.

Quando	Quem	O que fazer	O que registar
Todos os dias	Suporte	Conferir agentes offline inesperados, alertas importantes e falhas de backup.	PC, colaborador, hora, alerta e responsável.
Quando houver problema	Colaborador	Dizer o nome do PC e o que aconteceu. Autorizar a assistência conforme a política.	Mensagem exata e o momento em que começou.
Uma vez por semana	Suporte	Rever atualizações no piloto, pendências de análise e programas sem atualização.	Ações realizadas e pendências com data.
Entrada de colaborador	Suporte + responsável	Preparar PC, conta comum, agentes e aplicações licenciadas.	Nome VELOMA-PC-NNN, serial e responsável.
Saída de colaborador	Suporte + responsável	Revogar os acessos aplicáveis e preservar os dados da empresa.	Serviços revogados e destino dos dados.
Periodicamente	Responsável do cofre	Rever acessos privilegiados e, quando implantada, a auditoria de senhas.	Riscos e rotações, sem gravar senhas no relatório.

Quando algo não funciona

Sintoma	Primeira verificação
O nome da intranet não abre	VPN conectada e DNS do NAS disponível.
O painel abre, mas não aparece o PC	Agente certo, PC ligado e cadastro/rota validados.
Ecrã remoto preto ou sem controlo	Permissões do sistema, principalmente no macOS.
Wazuh mostra agente offline	Serviço do agente, conectividade e endereço do gestor.
Análise diz “não analisado”	Limites de tamanho/arquivo; encaminhar à TI.

15 · PRIMEIRO PILOTO

A forma certa de pôr em uso.

Antes de prometer gestão de todos os computadores, complete esta ficha com um Windows e um Mac.

EQUIPAMENTO _____ COLABORADOR _____
 DATA _____ RESPONSÁVEL _____

- ☐ Nome e número de série registados.
- ☐ Intranet acessível pela rede/VPN correta; certificado confiado.
- ☐ Agente MeshCentral instalado com endereço alcançável a partir da loja.
- ☐ PC aparece online; ecrã e ficheiros testados.
- ☐ Agente Wazuh cadastrado e ativo no gestor correto.
- ☐ Defender ativo no Windows; proteção do Mac e permissões revistas.
- ☐ Rotina de análise e tratamento dos ficheiros não analisados definida.
- ☐ Aplicações, licenças e atualizações verificadas.
- ☐ Backup configurado e pelo menos uma restauração de teste concluída.
- ☐ Contas e permissões entregues; senha temporária trocada.
- ☐ Colaborador sabe como pedir ajuda e reconhecer a sessão de suporte.

Depois do piloto

Repetir o processo por pequenos grupos. Cadastrar os agentes depois da instalação da imagem, com identidade única por computador. Só considerar “pronto” quando os testes tiverem resultado registado.

Agente

Pequeno programa instalado em cada PC para o ligar à central.

VPN

Ligação privada para alcançar a rede autorizada.

DNS

Traduz nomes como suporte.intra.veloma.app em endereços.

MFA

Segundo fator, além da senha, para confirmar a identidade.

16 · PARA O RESPONSÁVEL TÉCNICO

Referência e próximos passos.

Esta página ajuda a distinguir configuração disponível de trabalho ainda por concluir.

Assunto	Onde consultar / o que validar
Instaladores Wazuh	Hub: /windows/ e /macos/ . Scripts e pacotes separados por sistema. A instalação/cadastro precisa de rota válida ao gestor.
DNS da intranet em Windows	Hub: /windows/intranet/ . Script de DNS para estações fisicamente na loja. O HTTPS usa certificado público; não é necessário importar CA privada. Não aplicar o DNS da loja à LAN atual do MiniPC.
Perfil de trabalho Windows	Hub: /windows/workstation/ , instruções em DEPLOYMENT.txt . Perfil preparado; imagem/PXE e piloto não concluídos.
Relatório do Mac atual	~/Library/Application Support/VelomaAntivirus/last-report.json . Destinado ao suporte; não publicar caminhos de arquivos do colaborador.
Antivírus central	API em 8446 e análise de partilhas agendada para 02:30 na hora do servidor. O resultado refere-se apenas ao conteúdo efetivamente analisado.
Cadências Wazuh configuradas	Inventário por agente: 1 hora. Avaliação de configuração: 12 horas. Validação da central Windows: 5 minutos.
Rede e agentes da loja	Homologar os destinos/portas dos agentes; o proxy web da intranet não encaminha automaticamente os protocolos Wazuh.
Backups	UrBackup disponível. Ter servidor ativo não comprova cópia de cada PC; política, cliente, retenção e restauração precisam de teste.
SSO / Keycloak	Não há login único de produção confirmado para esta central. A instância identificada é local de desenvolvimento. Tratar as credenciais por serviço.

Prioridades de implantação

1. Distribuir o DNS da intranet na loja. 2. Homologar agentes em piloto. 3. Validar backup e restauração. 4. Distribuir por grupos. 5. Integrar a auditoria do cofre. 6. Concluir a imagem e o processo de instalação remota.

17 · FONTES E LIMITES

De onde vêm as instruções?

Configuração local observada + documentação oficial. Revisão: 23 de outubro de 2026.

MeshCentral — agentes e controlo remoto

docs.meshcentral.com/meshcentral/

Wazuh — agente e cadastro

documentation.wazuh.com/current/user-manual/agent/

ClamAV — motor, análise e limites

docs.clamav.net/manual/Usage/Scanning.html

Microsoft — Defender e Histórico de proteção

Microsoft Support · Virus and threat protection

Microsoft — requisitos de RDP

Microsoft Learn · Enable Remote Desktop

Microsoft — permissões de controlo remoto no macOS

Microsoft Learn · Deploy Remote Help · macOS

Have I Been Pwned — pesquisa de senhas por prefixo

haveibeenpwned.com/API/v3#PwnedPasswords

O que foi verificado para esta edição

Painéis web de suporte e segurança; serviços ClamAV, atualizações e API; dois agentes Wazuh ativos; DNS/VPN e relay do NAS; ficheiros de instalação publicados e último relatório do cliente do Mac.

As capturas são reais. As instruções de instalação dos postos são o roteiro para o piloto; não afirmam que todos os postos já receberam agentes. A auditoria do cofre, a imagem/PXE e o SSO de produção não foram implementados por este manual.



**Uma central útil é uma central
que a equipa sabe utilizar.**