# Política de Segurança da Informação da CallNet Solutions

## Sumário

1. **Política de Segurança da Informação da CallNet Solutions**
2. 1.1. Propósito
3. 1.2. Abrangência
4. 1.3. Princípios Orientadores
5. 1.4. Gestão de Acesso
6. 1.5. Segurança de Redes e Sistemas
7. 1.6. Segurança da Informação em Nuvem (AWS)
8. 1.7. Backup e Recuperação de Desastres
9. 1.8. Resposta a Incidentes de Segurança
10. 1.9. Conscientização e Treinamento
11. 1.10. Auditoria e Revisão
12. **Cartilha de Boas Práticas de Acesso Seguro para Colaboradores da CallNet Solutions**
13. 2.1. Senhas Fortes e Seguras
14. 2.2. Acesso à Rede e Sistemas
15. 2.3. E-mails e Phishing
16. 2.4. Proteção contra Malware
17. 2.5. Uso Consciente da Informação
18. **Mecanismos de Proteção, Rastreamento de Vulnerabilidades e Soluções de Atenuação**
19. 3.1. Mecanismos de Proteção à Integridade, Confidencialidade e Disponibilidade da Informação
20. 3.1.1. Proteção à Confidencialidade
21. 3.1.2. Proteção à Integridade
22. 3.1.3. Proteção à Disponibilidade
23. 3.2. Rastreamento de Possíveis Vulnerabilidades e Soluções de Atenuação
24. 3.2.1. Ferramentas de Exploração de Vulnerabilidades
25. 3.2.2. Possíveis Vulnerabilidades e Soluções de Atenuação

## 1. Política de Segurança da Informação da CallNet Solutions

### 1.1. Propósito

Esta Política de Segurança da Informação (PSI) estabelece as diretrizes e responsabilidades para a proteção dos ativos de informação da CallNet Solutions, garantindo a **confidencialidade**, **integridade** e **disponibilidade** dos dados. O objetivo é minimizar riscos, prevenir incidentes de segurança e assegurar a continuidade dos negócios.

### 1.2. Abrangência

Esta política se aplica a todos os funcionários, colaboradores, prestadores de serviço, parceiros e qualquer indivíduo que tenha acesso aos sistemas, redes e informações da CallNet Solutions, independentemente de sua localização (matriz, filiais ou trabalho remoto).

### 1.3. Princípios Orientadores

* **Confidencialidade**: As informações sensíveis e confidenciais da CallNet Solutions devem ser acessíveis apenas por indivíduos autorizados, de acordo com a necessidade do negócio.
* **Integridade**: As informações devem ser precisas, completas e protegidas contra modificações não autorizadas ou acidentais.
* **Disponibilidade**: Os sistemas e as informações críticas devem estar acessíveis e operacionais para os usuários autorizados sempre que necessário.
* **Conformidade**: Todas as atividades de segurança da informação devem estar em conformidade com as leis, regulamentações e padrões aplicáveis, bem como com os contratos e acordos comerciais.
* **Responsabilidade**: Todos os indivíduos são responsáveis por compreender e cumprir esta política e as diretrizes de segurança da informação.

### 1.4. Gestão de Acesso

* **Controle de Acesso Lógico**:
  + Acesso a sistemas e informações deve ser baseado no princípio do **menor privilégio**, concedendo apenas as permissões estritamente necessárias para o desempenho das funções.
  + Contas de usuário devem ser **pessoais e intransferíveis**. O compartilhamento de credenciais é estritamente proibido.
  + Senhas devem ser complexas (mínimo de 12 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais), alteradas periodicamente (a cada 90 dias) e nunca reutilizadas.
  + A autenticação de múltiplos fatores (MFA) será implementada sempre que possível para acesso a sistemas críticos e em nuvem (AWS).
  + Sessões inativas devem ser bloqueadas automaticamente após 15 minutos de inatividade.
* **Controle de Acesso Físico**:
  + O acesso físico às instalações da CallNet Solutions, incluindo salas de servidores e áreas restritas, será controlado por sistemas de acesso (cartões, biometria) e monitorado por câmeras de segurança.
  + Visitantes devem ser registrados e acompanhados por um funcionário da CallNet Solutions.

### 1.5. Segurança de Redes e Sistemas

* **Firewalls**: Todos os pontos de entrada e saída da rede devem ser protegidos por firewalls devidamente configurados para filtrar o tráfego não autorizado.
* **Segmentação de Rede**: A rede deve ser segmentada (LAN corporativa, Wi-Fi corporativo, Wi-Fi público) para isolar diferentes tipos de tráfego e limitar o impacto de possíveis incidentes.
* **VPN**: O acesso remoto à rede corporativa deve ser realizado exclusivamente por meio de VPNs seguras, garantindo a criptografia do tráfego.
* **Atualização de Software**: Todos os sistemas operacionais, aplicações e softwares devem ser mantidos atualizados com os patches de segurança mais recentes.
* **Antivírus e Antimalware**: Soluções de segurança de endpoint devem ser instaladas e mantidas atualizadas em todos os dispositivos da CallNet Solutions.
* **Configuração Segura**: Servidores (Windows Server 2025, Windows Server 2022) e demais equipamentos de rede devem ser configurados de acordo com as melhores práticas de segurança (hardened).

### 1.6. Segurança da Informação em Nuvem (AWS)

* **Responsabilidade Compartilhada**: A CallNet Solutions reconhece a responsabilidade compartilhada com a AWS pela segurança da informação, onde a AWS é responsável pela segurança *da* nuvem e a CallNet Solutions é responsável pela segurança *na* nuvem.
* **VPC e Sub-redes**: A utilização de VPCs e sub-redes privadas garante o isolamento e a segregação lógica dos recursos em nuvem.
* **Grupos de Segurança e NACLs**: As políticas de segurança serão aplicadas através de Grupos de Segurança e Network Access Control Lists (NACLs) para controlar o tráfego permitido e proibido.
* **Gerenciamento de Identidade e Acesso (IAM)**: Utilização do AWS IAM para gerenciar o acesso aos recursos em nuvem com o princípio do menor privilégio.
* **Criptografia**: Dados armazenados em instâncias EC2 e outros serviços AWS devem ser criptografados sempre que possível.
* **Backup e Recuperação de Desastres**: Implementação de rotinas de backup regulares e planos de recuperação de desastres para os dados em nuvem.

### 1.7. Backup e Recuperação de Desastres

* **Backup Regular**: Backups completos e incrementais de dados críticos devem ser realizados regularmente e armazenados em locais seguros e externos à rede principal.
* **Teste de Recuperação**: Os planos de recuperação de desastres e os procedimentos de restauração de backup devem ser testados periodicamente para garantir sua eficácia.

### 1.8. Resposta a Incidentes de Segurança

* **Plano de Resposta a Incidentes**: Um plano de resposta a incidentes será estabelecido para detectar, conter, erradicar e recuperar-se de incidentes de segurança de forma eficaz.
* **Comunicação**: Incidentes de segurança devem ser comunicados imediatamente à equipe de TI responsável.

### 1.9. Conscientização e Treinamento

* **Treinamento Regular**: Todos os funcionários receberão treinamento regular sobre as políticas de segurança da informação e as melhores práticas de segurança cibernética.
* **Conscientização**: Campanhas de conscientização serão realizadas para manter os funcionários informados sobre as ameaças e as melhores práticas de segurança.

### 1.10. Auditoria e Revisão

* **Auditorias Periódicas**: A segurança da informação será auditada periodicamente para identificar não conformidades e oportunidades de melhoria.
* **Revisão da Política**: Esta política será revisada anualmente ou sempre que houver mudanças significativas no ambiente de negócios ou tecnológico.

## 2. Cartilha de Boas Práticas de Acesso Seguro para Colaboradores da CallNet Solutions

A segurança da informação é responsabilidade de todos na CallNet Solutions! Siga estas boas práticas para proteger nossos dados e sistemas.

### 2.1. Senhas Fortes e Seguras

* **Crie senhas complexas**: Use no mínimo 12 caracteres, combinando letras maiúsculas e minúsculas, números e símbolos (ex: Puc@M!nas2025#).
* **Não use informações pessoais**: Evite datas de aniversário, nomes de pets, sequências simples (123456) ou palavras de dicionário.
* **Não reutilize senhas**: Cada serviço deve ter uma senha única.
* **Mude suas senhas regularmente**: Altere-as a cada 90 dias.
* **Nunca compartilhe suas senhas**: Elas são pessoais e intransferíveis.
* **Use um gerenciador de senhas**: Se precisar, utilize um gerenciador de senhas seguro.

### 2.2. Acesso à Rede e Sistemas

* **Acesso VPN para trabalho remoto**: Ao trabalhar de casa ou de outro local, sempre utilize a VPN (Virtual Private Network) da CallNet Solutions para acessar a rede e os sistemas corporativos. Isso criptografa sua conexão e a torna segura.
* **Redes Wi-Fi públicas**: Evite acessar informações confidenciais ou realizar transações bancárias em redes Wi-Fi públicas (aeroportos, cafés). Se precisar, utilize a VPN.
* **Bloqueie seu computador**: Sempre bloqueie sua tela (Windows + L) quando se afastar de seu computador, mesmo que por um curto período.
* **Não instale softwares não autorizados**: Não instale programas ou aplicativos sem a permissão da equipe de TI. Softwares não autorizados podem conter malwares ou vulnerabilidades. Todo o processo de instalação e requisição deve ser feito pelo time de infraestrutura.
* **Cuidado ao conectar dispositivos externos**: Antes de conectar pen drives, HDs externos ou outros dispositivos desconhecidos, certifique-se de que estão limpos e verifique-os com o antivírus.

### 2.3. E-mails e Phishing

* **Desconfie de e-mails suspeitos**: Fique atento a e-mails com erros de português, remetentes desconhecidos, pedidos urgentes de informações pessoais ou financeiras, ou anexos inesperados.
* **Não clique em links desconhecidos**: Não clique em links ou abra anexos de e-mails de remetentes que você não conhece ou que parecem suspeitos.
* **Verifique o remetente**: Antes de responder ou clicar, verifique cuidadosamente o endereço de e-mail do remetente para ter certeza de que é legítimo.
* **Reporte e-mails suspeitos**: Se você receber um e-mail que parece ser um golpe de phishing, encaminhe-o imediatamente para a equipe de TI e, em seguida, exclua-o.

### 2.4. Proteção contra Malware

* **Mantenha o antivírus ativado e atualizado**: Certifique-se de que o software antivírus da empresa esteja sempre funcionando e atualizado em seu computador.
* **Faça varreduras regulares**: Realize varreduras completas no seu computador periodicamente.
* **Cuidado com downloads**: Baixe arquivos apenas de fontes confiáveis.

### 2.5. Uso Consciente da Informação

* **Não compartilhe informações confidenciais**: Não discuta informações confidenciais da empresa em locais públicos ou em canais de comunicação não seguros.
* **Descarte seguro de informações**: Ao descartar documentos impressos com informações confidenciais, utilize um triturador de papel.
* **Reporte atividades suspeitas**: Se você notar qualquer atividade incomum em seu computador, rede ou conta, avise imediatamente a equipe de TI.

## 3. Mecanismos de Proteção, Rastreamento de Vulnerabilidades e Soluções de Atenuação

### 3.1. Mecanismos de Proteção à Integridade, Confidencialidade e Disponibilidade da Informação

A CallNet Solutions implementará uma série de ferramentas e configurações para garantir a segurança da informação, tanto no ambiente *On Premise* quanto *On Cloud*.

#### 3.1.1. Proteção à Confidencialidade

* **Criptografia de Dados**:
  + **Em trânsito**: Todo o tráfego entre a matriz e as filiais (via VPN SD-WAN/VPN) e o acesso remoto (VPN) será criptografado. O acesso a aplicações web (Intranet e Externas) será via HTTPS (TLS/SSL).
  + **Em repouso (AWS)**: Instâncias EC2 e volumes EBS em nuvem serão configurados com criptografia ativada.
* **Controle de Acesso Lógico (Active Directory e AWS IAM)**:
  + **Active Directory (On Premise)**: Centralização do gerenciamento de usuários, grupos e permissões, aplicando o princípio do menor privilégio. GPOs serão utilizadas para reforçar a segurança em todas as máquinas do domínio, como o bloqueio do Painel de Controle e configurações de senhas.
  + **AWS IAM (On Cloud)**: Gerenciamento de identidades e acessos granular para recursos em nuvem, garantindo que apenas usuários e serviços autorizados acessem os recursos AWS. Utilização de **MFA** para acesso à console AWS.
* **Segmentação de Rede**:
  + **VLANs (On Premise)**: Criação de VLANs para segregar a rede corporativa, rede de convidados (Wi-Fi público) e, se aplicável, rede de servidores, isolando o tráfego e limitando o alcance de potenciais ataques.
  + **VPC e Sub-redes (On Cloud)**: Utilização de uma Virtual Private Cloud (VPC) com sub-redes privadas para hospedar as aplicações, garantindo o isolamento da rede pública da internet.
* **Firewalls (On Premise e On Cloud)**:
  + **Firewall Dedicado (On Premise)**: Implementação de um firewall de borda na matriz para controle de tráfego de entrada e saída, com regras de filtragem de pacotes, inspeção de estado e prevenção de intrusões (IPS/IDS).
  + **Grupos de Segurança e NACLs (AWS)**: Aplicação de regras de firewall a nível de instância (Security Groups) e a nível de sub-rede (Network Access Control Lists) para controlar o tráfego de rede na nuvem, permitindo apenas as portas e protocolos essenciais.
* **Hardening de Sistemas**: Configuração de servidores (Windows Server 2025 e 2022) e estações de trabalho de acordo com as melhores práticas de segurança, desabilitando serviços desnecessários, configurando permissões adequadas e aplicando políticas de segurança.

#### 3.1.2. Proteção à Integridade

* **Controle de Versões e Backup de Configurações**:
  + Manutenção de controle de versões para configurações de rede e servidor, permitindo o rollback em caso de alterações não desejadas.
  + Backups regulares das configurações do Active Directory, DNS, DHCP e IIS.
* **Assinatura Digital e Hashing (IIS)**: Assegurar a integridade dos arquivos hospedados no IIS através de técnicas de hashing para verificar se os arquivos foram modificados.
* **Restrições de Alteração (GPOs)**: Políticas de Grupo no Active Directory para impedir que usuários finais alterem configurações críticas do sistema, como o bloqueio do Painel de Controle, garantindo a integridade do ambiente.
* **Controle de Acesso com Permissões de Gravação**: Limitar as permissões de gravação a diretórios e arquivos críticos apenas para usuários e processos autorizados.

#### 3.1.3. Proteção à Disponibilidade

* **Redundância e Alta Disponibilidade**:
  + **Servidores Críticos (On Premise)**: Para serviços críticos como Active Directory e DNS, considerar a implementação de controladores de domínio adicionais para redundância.
  + **Balanceamento de Carga (AWS)**: Se as aplicações em nuvem exigirem alta disponibilidade e escalabilidade, considerar a implementação de Load Balancers (ALB/NLB) para distribuir o tráfego entre múltiplas instâncias EC2.
  + **Zonas de Disponibilidade (AWS)**: Hospedar aplicações em nuvem em múltiplas Zonas de Disponibilidade da AWS para proteger contra falhas em um único data center.
* **Monitoramento de Performance e Recursos (Zabbix)**:
  + O Zabbix monitora o uso de CPU, memória, disco e status de serviços em ambos os ambientes (local e nuvem). Isso permite identificar gargalos, prever falhas e agir proativamente para evitar indisponibilidade.
  + **Alertas**: Configuração de alertas no Zabbix para notificar a equipe de TI sobre anomalias ou excedente de limites de recursos, permitindo uma resposta rápida.
* **Backups e Planos de Recuperação de Desastres**:
  + **Backup Regular**: Realização de backups regulares dos dados e configurações críticos, tanto no ambiente local quanto na nuvem.
  + **Teste de Recuperação**: Testes periódicos dos planos de recuperação de desastres e dos backups para garantir a capacidade de restauração e a continuidade dos negócios em caso de falhas ou ataques.

### 3.2. Rastreamento de Possíveis Vulnerabilidades e Soluções de Atenuação

Para identificar e mitigar vulnerabilidades, a CallNet Solutions adotará uma abordagem proativa.

#### 3.2.1. Ferramentas de Exploração de Vulnerabilidades

* **Scanners de Vulnerabilidade de Rede**:
  + **OpenVAS/Nessus**: Ferramentas como OpenVAS (open source) ou Nessus (comercial) serão utilizadas para realizar varreduras de vulnerabilidades na rede local e em alvos externos (IP público da AWS). Elas podem identificar portas abertas desnecessariamente, serviços desatualizados, configurações inadequadas, e potenciais vulnerabilidades em sistemas operacionais e aplicações.
  + **Frequência**: As varreduras serão realizadas mensalmente e sempre após grandes alterações na infraestrutura.
* **Scanners de Segurança de Aplicações Web (DAST)**:
  + **OWASP ZAP/Burp Suite (Community Edition)**: Para as aplicações web (Intranet e Aplicação Externa no IIS), scanners de segurança de aplicações web dinâmicos (DAST) podem ser utilizados para identificar vulnerabilidades comuns em aplicações web, como injeção de SQL, XSS, quebras de autenticação, etc.
  + **Frequência**: Varreduras quinzenais ou após cada nova funcionalidade desenvolvida.
* **Análise de Logs (Zabbix e Logs de Sistema)**:
  + O Zabbix pode ser configurado para coletar e analisar logs de segurança de servidores (Windows Event Logs) e dispositivos de rede. Padrões incomuns ou tentativas de acesso não autorizadas podem indicar atividades maliciosas.
  + **SIEM (Security Information and Event Management)**: Embora o Zabbix ofereça funcionalidades de log, para um ambiente mais complexo, a implementação de um SIEM (ex: ELK Stack - Elasticsearch, Logstash, Kibana) pode centralizar e correlacionar eventos de segurança de diversas fontes para detecção avançada de ameaças.
* **Ferramentas de Auditoria de Configuração (ex: PowerShell DSC)**:
  + Utilização de ferramentas de gerenciamento de configuração para garantir que as configurações dos servidores e dispositivos estejam em conformidade com as políticas de segurança e para identificar desvios.

#### 3.2.2. Possíveis Vulnerabilidades e Soluções de Atenuação

Com base na infraestrutura proposta, algumas vulnerabilidades comuns e suas atenuações são:

* **Vulnerabilidade**: **Ataques de Força Bruta contra o Active Directory/Servidores (On Premise)**
  + **Descrição**: Tentativas repetidas de adivinhar senhas de usuários ou administradores.
  + **Atenuação**:
    - **Política de Bloqueio de Conta**: Configurar no Active Directory uma política de bloqueio de conta após um número X de tentativas falhas de login (ex: 3 a 5 tentativas) por um período de tempo Y (ex: 30 minutos).
    - **Complexidade de Senha**: Impor senhas complexas e longas.
    - **MFA**: Se possível, implementar MFA para acesso administrativo.
    - **Monitoramento de Logs**: Monitorar logs de segurança para tentativas de login falhas e configurar alertas no Zabbix.
* **Vulnerabilidade**: **Ataques de Phishing/Engenharia Social (Geral)**
  + **Descrição**: Tentativas de enganar usuários para que revelem informações confidenciais ou instalem malware. Esses ataques podem ser genéricos ou altamente personalizados (spear phishing), utilizando informações coletadas de fontes abertas (OSINT), como o cargo de um funcionário no LinkedIn ou detalhes sobre projetos da empresa, para aumentar a credibilidade da fraude.
  + **Atenuação**:
    - **Treinamento e Conscientização**: Educação contínua dos colaboradores sobre como identificar e reportar e-mails de phishing e outras táticas de engenharia social. Os treinamentos devem incluir exemplos práticos de como suas informações pessoais e profissionais publicadas online podem ser usadas para criar ataques direcionados contra eles e a empresa.
    - **Simulações de Ataques Direcionados:** Além de campanhas de phishing genéricas, realizar simulações periódicas de *spear phishing*, utilizando informações publicamente disponíveis para testar a resiliência dos colaboradores a ataques personalizados.
    - **Filtros de Spam e Antivírus**: Implementar e manter atualizados filtros de spam e soluções antivírus/antimalware nos e-mails e endpoints.
    - **Autenticação de Múltiplos Fatores (MFA)**: Implementar MFA para todos os serviços acessíveis externamente.
* **Vulnerabilidade**: **Acesso Não Autorizado via RDP (On Cloud)**
  + **Descrição**: Tentativas de acesso não autorizado à instância EC2 via Remote Desktop Protocol (RDP), especialmente se a porta estiver aberta para o mundo.
  + **Atenuação**:
    - **Restrição de IP no Security Group**: Limitar o acesso RDP (porta 3389) no Grupo de Segurança da AWS apenas aos IPs da rede corporativa da CallNet Solutions ou a IPs de VPNs seguras, e não 0.0.0.0/0.
    - **Chaves .pem**: Manter a autenticação por chave .pem segura.
    - **Renomear Usuário Administrador**: Renomear a conta "Administrator" da instância.
    - **Bloqueio de Contas e Senhas Fortes**: Implementar políticas de bloqueio de contas e exigir senhas fortes para usuários RDP.
* **Vulnerabilidade**: **Vulnerabilidades em Aplicações Web (IIS - On Premise e On Cloud)**
  + **Descrição**: Falhas de segurança no código ou configuração das aplicações hospedadas no IIS (SQL Injection, XSS, etc.).
  + **Atenuação**:
    - **Desenvolvimento Seguro**: Adotar práticas de desenvolvimento seguro (SDLC) para minimizar vulnerabilidades no código das aplicações.
    - **WAF (Web Application Firewall)**: Para a aplicação externa (AWS), considerar a implementação de um AWS WAF para proteger contra ataques comuns da web. Para a intranet, um WAF de software ou hardware.
    - **Atualização do IIS e Frameworks**: Manter o IIS e os frameworks de desenvolvimento (ex: .NET) atualizados com os patches de segurança mais recentes.
    - **Varreduras Regulares de Aplicações Web (DAST/SAST)**: Realizar varreduras regulares de segurança nas aplicações.
* **Vulnerabilidade**: **Configurações Inadequadas de Firewalls/Grupos de Segurança (Geral)**
  + **Descrição**: Regras de firewall muito permissivas, permitindo tráfego desnecessário ou expondo serviços.
  + **Atenuação**:
    - **Princípio do Menor Privilégio**: Configurar as regras de firewall (tanto no firewall de borda local quanto nos Security Groups/NACLs da AWS) para permitir apenas o tráfego essencial e necessário.
    - **Revisão Periódica**: Realizar revisões regulares das regras de firewall para remover as desnecessárias e garantir a conformidade.
    - **Testes de Penetração (Pen Test)**: Realizar testes de penetração periódicos para simular ataques e identificar vulnerabilidades não detectadas por scanners.
* **Vulnerabilidade**: **Vulnerabilidades em Sistemas Operacionais e Software (Geral)**
  + **Descrição**: Falhas de segurança conhecidas em sistemas operacionais (Windows Server 2025/2022, Windows 11) ou softwares instalados.
  + **Atenuação**:
    - **Gerenciamento de Patches**: Implementar um robusto processo de gerenciamento de patches para aplicar atualizações de segurança em todos os sistemas operacionais e softwares o mais rápido possível após seu lançamento.
    - **Remoção de Software Desnecessário**: Desinstalar softwares e serviços que não são essenciais para a operação, minimizando a superfície de ataque.
    - **Hardening**: Aplicar configurações de segurança (hardening) em todos os sistemas.
* **Vulnerabilidade: Exposição de Informações Sensíveis em Fontes Abertas (OSINT)**
* **Descrição:** Coleta de informações sobre funcionários, tecnologias internas e processos da CallNet Solutions a partir de fontes públicas como redes sociais (LinkedIn, Facebook, etc.), sites de anúncios de emprego, artigos de notícias e fóruns. Um ator malicioso pode usar esses dados para mapear a estrutura organizacional, identificar a tecnologia utilizada (ex: versões de Windows Server, AWS, sistemas de CRM) e selecionar alvos para ataques de engenharia social altamente direcionados (Spear Phishing e Vishing).
* **Atenuação:**
  + **Política de Uso de Redes Sociais:** Implementar e comunicar uma política clara que oriente os colaboradores sobre a divulgação de informações relacionadas ao trabalho em suas redes sociais pessoais. Recomendar que não publiquem fotos de crachás, telas de sistemas internos ou detalhes sobre a hierarquia e projetos da empresa.
  + **Higienização de Anúncios de Vagas:** Revisar os anúncios de emprego para remover detalhes técnicos excessivos sobre a infraestrutura que não são essenciais para a qualificação do candidato. Por exemplo, em vez de "experiência com Windows Server 2025 e Zabbix", optar por "experiência com administração de servidores Windows e ferramentas de monitoramento de infraestrutura".
  + **Monitoramento da Pegada Digital:** Realizar um monitoramento periódico da presença online da empresa e de seus principais colaboradores para identificar exposições não intencionais de dados que possam ser exploradas.
  + **Treinamento Específico sobre Vishing:** Dado o ambiente de call center, realizar treinamentos focados em Vishing (phishing por voz), simulando cenários em que um atacante se passa por um colega ou suporte técnico, utilizando informações coletadas via OSINT (ex: nome de um supervisor, um problema técnico recente) para obter credenciais ou acesso.

Ao implementar e manter esses mecanismos de proteção e realizar o rastreamento de vulnerabilidades com as ferramentas e estratégias descritas, a CallNet Solutions estará fortalecendo significativamente sua postura de segurança cibernética, protegendo seus ativos de informação e garantindo a continuidade de suas operações.

## Glossário

* **Active Directory (AD):** Serviço de diretório da Microsoft para gerenciamento de usuários, computadores e outros recursos em uma rede Windows.
* **Antimalware:** Software projetado para detectar, prevenir e remover softwares maliciosos.
* **Antivírus:** Software que detecta e remove vírus de computador.
* **AWS (Amazon Web Services):** Plataforma de computação em nuvem que oferece uma ampla gama de serviços.
* **Confidencialidade:** Princípio de segurança da informação que garante que os dados sejam acessíveis apenas por indivíduos ou sistemas autorizados.
* **Criptografia:** Processo de conversão de informações em um código para impedir o acesso não autorizado.
* **DAST (Dynamic Application Security Testing):** Metodologia de teste de segurança que analisa aplicações em execução para identificar vulnerabilidades.
* **Disponibilidade:** Princípio de segurança da informação que assegura que os sistemas e dados estejam acessíveis e funcionais quando necessário.
* **Firewall:** Sistema de segurança de rede que monitora e controla o tráfego de rede de entrada e saída com base em regras de segurança predefinidas.
* **GPO (Group Policy Object):** Objeto no Active Directory que contém configurações para usuários e computadores, usadas para aplicar políticas de segurança.
* **Hardening:** Processo de fortalecer a segurança de um sistema, removendo serviços desnecessários, aplicando patches e configurando permissões.
* **IAM (Identity and Access Management):** Serviço que permite gerenciar identidades digitais e controlar o acesso a recursos em nuvem ou locais.
* **IIS (Internet Information Services):** Servidor web da Microsoft, usado para hospedar sites e aplicações web.
* **Integridade:** Princípio de segurança da informação que garante que os dados sejam precisos, completos e protegidos contra alterações não autorizadas.
* **IPS/IDS (Intrusion Prevention System/Intrusion Detection System):** Sistemas que monitoram o tráfego de rede em busca de atividades maliciosas, podendo bloquear ou alertar sobre ataques.
* **Malware:** Termo genérico para software malicioso, como vírus, worms, cavalos de Troia e ransomware.
* **MFA (Autenticação de Múltiplos Fatores):** Método de autenticação que exige que o usuário forneça duas ou mais evidências (fatores) para verificar sua identidade.
* **NACLs (Network Access Control Lists):** Listas de controle de acesso de rede, usadas na AWS para controlar o tráfego de entrada e saída de sub-redes.
* **Nessus:** Ferramenta comercial de varredura de vulnerabilidades amplamente utilizada.
* **OpenVAS:** Ferramenta de varredura de vulnerabilidades de código aberto.
* **Patches:** Atualizações de software lançadas para corrigir bugs, vulnerabilidades de segurança ou melhorar funcionalidades.
* **Pen Test (Teste de Penetração):** Simulação de um ataque cibernético autorizado contra um sistema de computador para avaliar sua segurança.
* **Phishing:** Tipo de ataque de engenharia social onde criminosos tentam enganar indivíduos para obter informações confidenciais, como senhas, por meio de e-mails ou mensagens falsas.
* **PSI (Política de Segurança da Informação):** Documento que estabelece as diretrizes e regras para proteger os ativos de informação de uma organização.
* **RDP (Remote Desktop Protocol):** Protocolo de rede que permite a um usuário controlar um computador remotamente.
* **SDLC (Software Development Life Cycle):** Processo que abrange todas as fases do desenvolvimento de software, desde a concepção até a manutenção.
* **Security Groups:** Firewalls virtuais que controlam o tráfego de entrada e saída de instâncias em nuvem (AWS EC2).
* **Segmentação de Rede:** Divisão de uma rede em sub-redes menores para melhorar o desempenho e a segurança, isolando o tráfego.
* **SIEM (Security Information and Event Management):** Solução que coleta, normaliza e correlaciona eventos de segurança de várias fontes para detecção e análise de ameaças.
* **SQL Injection:** Técnica de ataque de injeção de código malicioso em aplicações web para manipular bancos de dados.
* **VLAN (Virtual Local Area Network):** Rede local virtual que permite agrupar dispositivos em uma mesma rede lógica, independentemente de sua localização física.
* **VPN (Virtual Private Network):** Rede privada virtual que cria uma conexão segura e criptografada sobre uma rede pública, como a internet.
* **VPC (Virtual Private Cloud):** Seção isolada logicamente na nuvem (AWS) onde o usuário pode lançar recursos AWS.
* **WAF (Web Application Firewall):** Firewall projetado para proteger aplicações web contra ataques comuns da web, como SQL Injection e XSS.
* **XSS (Cross-Site Scripting):** Vulnerabilidade de segurança em aplicações web que permite a um atacante injetar scripts maliciosos em páginas web visualizadas por outros usuários.
* **Zabbix:** Ferramenta de monitoramento de código aberto para redes, servidores e aplicações.