POLÍTICA DE SEGURANÇA CIBERNÉTICA E PLANO DE CONTINUIDADE DE NEGÓCIOS

OBJETIVO E ABRANGÊNCIA

1. Esta Política tem como objetivo disciplinar as ações voltadas à preservação da segurança da informação no âmbito das atividades desenvolvidas pela VIRTUS NEXUS e garantir a **confidencialidade, integridade e disponibilidade** das informações, protegendo os dados contra acessos não autorizados, vazamentos e incidentes de segurança que possam comprometer a operação e a reputação da empresa.

2. A VIRTUS NEXUS adota uma abordagem rigorosa para garantir a proteção das suas informações e a segurança cibernética dos seus sistemas. Esta política se aplica a todos os colaboradores, prestadores de serviço, parceiros e qualquer pessoa ou entidade que tenha acesso aos ativos de informação da empresa.

DIRETRIZES GERAIS

3. Todos os usuários devem:

    - Proteger os dados da VIRTUS NEXUS contra acessos indevidos e uso indevido.
    - Manter a confidencialidade das informações sensíveis, compartilhando apenas com quem tiver necessidade legítima.
    - Seguir as normas estabelecidas para uso de tecnologia, sistemas e dispositivos.
    - Reportar incidentes de segurança imediatamente para a área responsável.

CLASSIFICAÇÃO DA INFORMAÇÃO

4. Para garantir a proteção adequada, as informações da VIRTUS NEXUS são classificadas em três níveis:

    - Pública: pode ser acessada e compartilhada sem restrições.
    - Restrita: disponível apenas para colaboradores autorizados e parceiros estratégicos.
    - Confidencial: inclui dados estratégicos, financeiros e operacionais, sendo acessível somente a indivíduos autorizados.

SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE SISTEMAS

5. Medidas de Prevenção

A VIRTUS NEXUS adota as seguintes práticas de segurança cibernética:

- Controle de Acesso: Apenas usuários autorizados têm permissão para acessar informações críticas.
- Uso de Senhas Fortes: Senhas devem ser complexas e alteradas periodicamente.
- Autenticação de Dois Fatores: Aplicada para acessos sensíveis e sistemas essenciais.

- Monitoramento e Auditoria: Acesso a sistemas e dados críticos é registrado e monitorado regularmente.
- Backup Regular: Realização de cópias de segurança diárias para mitigar riscos de perda de dados.
- Proteção contra Ameaças: Sistemas de firewall, antivírus e anti-spam devem estar sempre atualizados.

6. Uso de Dispositivos e Softwares

- Apenas equipamentos corporativos devem ser usados para acessar sistemas da VIRTUS NEXUS.
- Instalação de softwares deve ser feita apenas por pessoal autorizado.
- Dispositivos pessoais não devem ser conectados à rede corporativa sem autorização formal.

7. Segurança na Comunicação

- É proibido o envio de informações confidenciais via e-mail pessoal ou aplicativos não autorizados.
- Mensagens suspeitas (phishing, spam) devem ser reportadas imediatamente.
- O acesso remoto aos sistemas da VIRTUS NEXUS deve ser feito somente por meio de VPN segura.

8. Monitoramento e Testes Periódicos

A VIRTUS NEXUS realizará auditorias periódicas para avaliar e aprimorar a segurança da informação. Testes de vulnerabilidade e simulações de ataques cibernéticos serão conduzidos regularmente para garantir a resiliência da empresa contra ameaças digitais.

9. Plano de Resposta a Incidentes

Em caso de incidente de segurança, serão adotadas as seguintes ações:

- Identificação e contenção do incidente.
- Investigação da origem e impacto do evento.
- Mitigação de danos e implementação de medidas corretivas.
- Notificação às partes afetadas, se necessário.
- Registro e documentação do incidente para análise futura.

10. Conscientização e Treinamento

Todos os colaboradores devem passar por treinamentos regulares sobre segurança da informação e boas práticas para evitar ameaças cibernéticas.

PLANO DE CONTINUIDADE DE NEGÓCIOS

A VIRTUS NEXUS adota uma infraestrutura 100% em nuvem, garantindo alta disponibilidade e resiliência operacional. No entanto, falhas tecnológicas, desastres naturais e eventos inesperados podem impactar as operações. Este plano tem como objetivo minimizar interrupções e garantir a rápida retomada das atividades em caso de incidentes.

11. Princípios do Plano de Continuidade

O Plano de Continuidade de Negócios (PCN) é baseado nos seguintes princípios:

- Disponibilidade: Garantia de que os serviços essenciais permaneçam acessíveis.
- Redundância: Infraestrutura distribuída para evitar pontos únicos de falha.
- Rapidez na recuperação: Procedimentos para retomada das operações no menor tempo possível.
- Segurança: Proteção dos dados e ativos críticos durante qualquer incidente.

12. Cenários de Interrupção e Respostas

Cenário	Impacto Potencial	Solução/Resposta
Falha em computador individual	Colaborador impossibilitado de acessar sistemas	Utilização de dispositivos alternativos (notebook reserva ou acesso via celular/tablet) e recuperação via credenciais na nuvem.
Falta de energia elétrica	Escritório sem acesso à internet e computadores desligados	Utilização de notebooks com bateria, conexão via rede 4G/5G e acesso remoto à infraestrutura na nuvem.
Indisponibilidade da internet	Equipe sem acesso aos sistemas baseados em nuvem	Uso de backup de conexão 4G/5G; opção de trabalho remoto emergencial.
Incêndio no escritório	Equipamentos físicos danificados; necessidade de realocação	Como todos os sistemas estão na nuvem, operação pode ser retomada remotamente de qualquer local seguro.
Ataque cibernético	Acesso não autorizado, vazamento de dados	Isolamento da ameaça, acionamento do time de segurança, recuperação de dados por backups, redefinição de acessos.
Falha na nuvem (AWS, Azure, Office 365)	Indisponibilidade temporária de serviços	Ativação de ambientes redundantes e failover automático para provedores alternativos caso necessário.

13. Estratégia de Recuperação

A VIRTUS NEXUS adota uma abordagem de recuperação em camadas, permitindo a retomada das atividades com base no nível de criticidade:

- Recuperação imediata (até 1h): soluções alternativas como conexões móveis, dispositivos reserva e suporte técnico imediato.
- Recuperação intermediária (até 24h): reinstalação de sistemas em novos dispositivos, ativação de backup de internet e acionamento de contingência para trabalho remoto.
- Recuperação avançada (até 48h): restauração completa da infraestrutura, avaliação dos impactos e revisão de estratégias para evitar recorrência.

14. Testes e Atualizações do Plano

Para garantir a eficácia do PCN, serão realizados:

- Testes semestrais de simulação de incidentes para avaliar a resposta e aprimorar estratégias.
- Auditorias anuais para revisar processos e identificar melhorias.

- Treinamentos periódicos para que toda a equipe saiba como agir em caso de falha.

15. Comunicação Durante Crises

Em caso de incidente relevante, será ativado um plano de comunicação interna e externa:

- Colaboradores: Notificação via e-mail, mensagens instantâneas e reunião emergencial online.
- Clientes e parceiros: Atualizações transparentes sobre impactos e medidas adotadas.
- Provedores de tecnologia: Acionamento imediato para suporte técnico e mitigação do problema.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada periodicamente e eventuais alterações serão feitas caso seja constatada necessidade de atualização do seu conteúdo. Poderá, também, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Versão	Data	Modificado por	Alterações
1.0	Agosto/2024	Virtus Nexus	Primeira Versão
1.1	Fev/2025	Virtus Nexus	Revisão geral da política de segurança da informação e inclusão do Plano de Continuidade