NEBRASKA
CAPITAL

# POLÍTICA DE SEGURANÇA CIBERNÉTICA

Outubro 2023
Elaboração: Diretor de Risco e Compliance
Revisão: Comitê de Risco e Compliance
Aprovação: Comitê de Gestão
2ª Versão
Vigência: 10/2025

Avenida Carlos Gomes, 400/703
Porto Alegre/RS - CEP 90.480-900
www.nebraskacapital.com.br

**SUMÁRIO**

## CONTROLE DE VERSÕES

| Data | Autor | Aprovado por | Versão | Modificações |
|---|---|---|---|---|
| 31/07/2021 | Bruno Claudino<br>Diretor de Risco e Compliance | Comitê de Gestão | 1.0 | 1ª Versão |
| 31/10/2023 | Alexandre Carlos Cunha<br>Diretor de Risco e Compliance | Comitê de Gestão | 2.0 | 2ª Versão |

**Figura 1 - Registro de Mudanças**

## 1. ESCOPO

1.1. Escopo. Serve o presente documento de Política de Segurança Cibernética da Nebraska Capital Gestão de Recursos Ltda. ("Nebraska Capital") para descrever detalhadamente a avaliação de riscos, ativos relevantes e suas possíveis falhas de sistema e o plano de resposta que os Integrantes da Nebraska Capital devem tomar para saná-los ou amenizá-los. As ações de proteção e prevenção visa mitigar os riscos identificados;

1.2. Cenários projetados. Assim, em que pese a Nebraska Capital possua lista com os nomes e telefones dos fornecedores de tecnologia da informação para solucionarem os problemas no menor tempo possível em caso de necessidade, os seguintes cenários são passíveis de falha e ações de Contingência:

| FALHA | RESPONSÁVEL DIRETO | PREVENÇÃO DA GESTORA |
|---|---|---|
| FALTA ENERGIA ELÉTRICA | BACK OFFICE | Em caso de falta de energia, os computadores e servidores da Nebraska Capital contam com sistemas de Nobreak com capacidade de 120 minutos de autonomia, o que permite gravar e salvar quaisquer tipos de arquivos ou informações que estavam sendo processadas no momento da falta de energia elétrica, bem como permitir que as atividades se mantenham por período razoável para que se reestabeleça a energia. |
| VÍRUS | BACK OFFICE | Todos os computadores da empresa são equipados com antivírus McaFee para eventuais ameaças e é feita de forma periódica e automática a varredura de todos os arquivos e e-mails dos computadores. |
| Hacker | BACK OFFICE | Temos um equipamento moderno de FireWall, no qual bloqueia e mitiga o risco de eventuais acessos não autorizados em nossas redes e arquivos; temos também uma rede dedicada para empregados e outra para eventuais visitantes para bloquear e mitigar o acesso aos arquivos. |
| Problemas com o servidor físico | BACK OFFICE | Em caso de problemas com o servidor físico, seja incêndio ou mau funcionamento, temos uma conta com a capacidade de 1 TB com a cópia de todos os arquivos da empresa. Este acesso é feito por senhas e esta senha é detida pelo diretor. |
| COMPUTADORES DANIFICADOS | BACK OFFICE | Em caso de problemas com os computadores utilizados pelos integrantes da Nebraska Capital, contamos com um sistema de Back UP on line via nuvens, o qual é atualizado no mínimo diariamente. |
| Falhas em geral | BACK OFFICE | Possuímos uma equipe terceirizada que presta atendimento 24 horas por dia caso tenhamos problemas nos equipamentos ou sistemas da empresa. |

## 2. CONTROLE DE ACESSO

2.1. Controle de Acesso. A Nebraska Capital adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A Nebraska Capital trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

2.2. Rastreabilidade. Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados. Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Nebraska Capital realiza configurações seguras de seus recursos. São feitos testes em ambiente de homologações e de prova de conceito antes do envio à produção.

2.3. Proteção contra tentativas de invasão. A Nebraska Capital conta com recursos anti malware em estações e servidores de rede, como antivírus e firewalls pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

2.4. Política de Senhas. A Nebraska adota uma padronização de senhas que prevê a necessidade dos seguintes critérios: uma letra maiúscula, um numeral e um caractere especial. Além disso, sempre que possível, deve ser adotada a autenticação multifator.

## 3. TESTES

3.1. Periodicidade dos Testes. A validação dos testes é feita a cada 24 meses (vinte e quatro), ou na eventual alteração da regulamentação referente a segurança cibernética testando a capacidade dos equipamentos e procedimentos a fim de entregar de modo satisfatório a integridade do sistema, tanto via digital físico ou nas nuvens para que seja atestado a manutenção da integridade do sistema;

3.2. Coordenação. A coordenação indireta da equipe de *Back office* (responsável direto) e das atividades relacionadas a esta Política de Segurança Cibernética será uma atribuição do Diretor de Compliance, a quem caberá realizar os treinamentos necessários, bem como os testes supramencionados.

3.3. Equipe externa. A Nebraska Capital optou por não manter equipe própria dedicada à segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (e.g. instalações, substituições, configurações), verificações e manutenções periódicas. Assim sendo, para implementação e monitoramento do contínuo da presente Política, a Nebraska Capital conta com o suporte e assessoria de empresa terceirizada de tecnologia da informação. Dessa mesma maneira, a Gestora não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética, em que pese o Back office seja devidamente treinado para lidar com as situações supramencionadas.

***