



Norma Interna – Uso da VPN

Fevereiro - 2023

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 2 de 8	Revisão: 02	Publicação: 02/2023

Sumário

1 – APRESENTAÇÃO..... 3

2 - FORMATO 3

3 - OBJETIVO..... 3

4 - ABRANGÊNCIA..... 3

5 - TERMOS E DEFINIÇÕES 3

6 - RESPONSABILIDADES 4

7 - DIRETRIZES 6

8 – GERENCIAMENTO VPN - AUTENTICAÇÃO DE USUÁRIOS..... 7

9 – MONITORAMENTO E REVISÃO..... 8

10 - CONSIDERAÇÕES FINAIS 8

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 3 de 8	Revisão: 02	Publicação: 02/2023

Responsável:	Emilson Queiroz (Gerente de TI)
Aprovado por:	Suleiman Bragança (CEO)
Políticas Relacionadas:	Política de Segurança da Informação
Data de Aprovação:	02/2023
Data de Revisão:	04/2024
Versão atual:	2.0

1 – APRESENTAÇÃO

A presente Norma está de acordo com as diretrizes da Política da Segurança da Informação da Vector.

2 - FORMATO

O documento é estruturado em torno de “diretrizes”, recomendações de boas práticas, a serem seguidas, em cada um dos tópicos listados nesse documento.

3 - OBJETIVO

O objetivo desse documento é normatizar o acesso remoto aos sistemas e demais recursos da rede da Vector. Esse documento enfatiza a importância de proteger as informações confidenciais transmitidas através do acesso remoto originados de redes externas.

4 - ABRANGÊNCIA

Esta Norma estabelece regras, que devem ser cumpridas por todos os colaboradores da Vector que utilizam a VPN.

5 - TERMOS E DEFINIÇÕES

Para efeito desta Norma aplicam-se os seguintes conceitos e definições:

- Segurança da Informação - proteção da informação contra ameaças para garantir a continuidade das atividades, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas na Vector.

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 4 de 8	Revisão: 02	Publicação: 02/2023

- Incidente em Segurança da Informação - qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações da instituição ou ameaçar a segurança da informação.
- Usuário – todos os colaboradores da Vector.
- VPN – a sigla VPN vem do inglês *V/r/u'a/ Private Network*, que em tradução livre significa Rede Virtual Privada. Ela utiliza a *internet* para se conectar a uma determinada localidade e assim poder usar seus serviços.

6 - RESPONSABILIDADES

Usuário:

- Manter sigilo das informações de acesso ao ambiente de rede da Vector e da conexão remota, sendo de sua total e exclusiva responsabilidade qualquer operação realizada por meio de suas credenciais de acesso.
- Comunicar imediatamente à área de Segurança da Informação da Vector qualquer situação que coloque em risco o acesso ao ambiente da rede de dados da Vector.
- Informar seu gestor quando forem identificados direitos de acesso remoto desnecessários à execução dessas atividades.

Gestor:

- Solicitar e/ou revogar as credenciais de acesso remoto dos usuários sob sua gestão.
- Conscientizar os usuários em seu domínio administrativo quanto às orientações presentes neste documento e nas boas práticas de segurança.
- Comunicar imediatamente ao setor de Segurança da Informação da Vector caso verifique qualquer ameaça, vulnerabilidade ou situação que possa colocar em risco o ambiente computacional em questão.
- Manter atualizada relação de usuários e seus papéis para que, de forma contínua, seja verificada a política de acessos mínimos e com isso a adequação dos perfis de acesso dos respectivos usuários.

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 5 de 8	Revisão: 02	Publicação: 02/2023

TI e Responsáveis pela Segurança da Informação:

- Administrar os acessos remotos ao ambiente de rede de dados da Vector.
- Manter a disponibilidade, integridade e confidencialidade em todo o ambiente de rede.
- Monitorar todo o ambiente de modo a identificar proativamente anomalias e acessos maliciosos.
- Manter os registros de acesso para fins de auditoria respeitando a legislação e as boas práticas de mercado.
- Manter mecanismos de segregação de acesso Lógico entre os ambientes de acesso remoto e os recursos computacionais em ambiente de rede local controlando o acesso por meio de políticas de acessos mínimos.
- Manter registro histórico de solicitações de criação e revogação de usuários para fins de auditoria e controle.
- Efetuar auditorias no ambiente como forma de garantir que os mecanismos de segurança adotados se mantêm eficientes.

RH

- Notificar à equipe de TI – Segurança da Informação da Vector a criação de credenciais de acesso remoto de funcionários admitidos.
- Notificar à equipe de TI – Segurança da Informação da Vector a revogação de credenciais de acesso remoto de funcionários que entrarem em licenças sem vencimento, desligamento definitivo, desligamento temporário por decisão judicial, afastamentos por licença de saúde.
- Conscientizar os novos funcionários quanto às orientações presentes neste documento e nas boas práticas de segurança.

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 6 de 8	Revisão: 02	Publicação: 02/2023

7 - DIRETRIZES

- Todos os computadores conectados às redes internas da Vector via VPN devem estar com as versões mais atualizadas de softwares antivírus, e com os últimos “patches” de segurança instalados.
- Estabelecer somente uma única conexão VPN com a rede da Vector.
- Utilizar equipamentos com sistemas operacionais compatíveis com a infraestrutura de computação da Vector.
- Não alterar, sem prévio consentimento, a configuração default da VPN fornecida pela Área de TI a Vector.
- O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.
- É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja.
- O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento. Por isso, deve o usuário manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.
- Importante o usuário nunca deve deixar sessões VPN abertas (logadas). Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 7 de 8	Revisão: 02	Publicação: 02/2023

8 – GERENCIAMENTO VPN - AUTENTICAÇÃO DE USUÁRIOS

A Vector implementou uma infraestrutura de VPN de última geração, utilizando especificamente a solução Cloudflare WARP.

Esta solução foi projetada para garantir que rede interna da Vector permaneça inacessível externamente, permitindo apenas a exposição seletiva de portas de servidores ou serviços via NAT/Firewall para usuários ou grupos específicos. Tal abordagem minimiza significativamente os riscos associados ao escaneamento de IPs e portas de rede.


O acesso dos usuários à rede da Vector é cuidadosamente controlado através da VPN, sendo concedida autorização exclusivamente para o uso de um serviço de Desktop Remoto específico. Este acesso é delimitado de forma rigorosa, vedando qualquer forma de compartilhamento de arquivos ou clipboard entre a máquina do usuário e quaisquer ambientes externos, com a exceção de sistemas previamente autorizados para uso interno. A Vector adota protocolos de restrição equivalentes tanto no ambiente do Desktop Remoto quanto nas estações de trabalho dos usuários, assegurando consistência nas medidas de segurança aplicadas.

A autenticação para a VPN, assim como para outras ferramentas e sistemas utilizados na rede da Vector, é centralizada por meio de um sistema de Single Sign-On (SSO), gerenciado na plataforma em nuvem da Jumpcloud.

Esse sistema adere estritamente a todos os protocolos de segurança estabelecidos, incluindo a exigência de senhas robustas e a implementação de autenticação multifatorial (MFA).

Para manter a integridade e a segurança da rede da Vector, e produzido registros detalhados em todas as camadas relevantes, incluindo processos de autenticação, atividades do firewall e registros de acesso.

Essas práticas são essenciais não apenas para atender às políticas de segurança da Vector, mas também para prover documentação abrangente durante processos de auditoria.

	Norma Interna – Uso da VPN	Última Revisão – 04/2024		
		Página 8 de 8	Revisão: 02	Publicação: 02/2023

9 – MONITORAMENTO E REVISÃO

A empresa reserva-se o direito de monitorar o uso da VPN para garantir a conformidade com a PSI.

A PSI deve ser revisada periodicamente para refletir as mudanças nas tecnologias e ameaças à segurança.

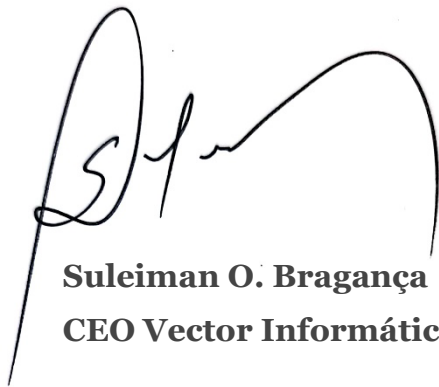
10 - CONSIDERAÇÕES FINAIS

As dúvidas decorrentes, de fatos não descritos nesta, deverão ser encaminhadas ao responsável pela TI Segurança da Informação.

A violação desta política por qualquer usuário será reportada à Direção da Vector que poderá tomar medidas para suspender de forma imediata, temporária ou permanente os seus privilégios de acesso a infraestrutura computacional da empresa, e podem também ocorrer ações legais contra o infrator.

Esta Norma entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Direção, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

Barueri, fevereiro de 2023



Suleiman O. Bragança
CEO Vector Informática Ltda.