





**COMPLEMENTO DA PSI -
GESTÃO DE IDENTIDADE E
CONTROLE DE ACESSO**

NOVEMBRO - 2021

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 2 de 18	Revisão: 03	Publicação: 09/2021

Sumário

1 – INTRODUÇÃO.....	3
2 - OBJETIVO.....	4
3 - ABRAGÊNCIA.....	4
4 - REFERÊNCIAS.....	4
5 - DEFINIÇÕES	4
6 – PRINCÍPIOS	6
7 – DESCRIÇÃO	7
7.1 – CONTROLE DE ACESSO LÓGICO	7
7.1.1- Papéis e Responsabilidades.....	7
7.1.2- Detalhamento	9
7.2 – SEGURANÇA FÍSICA	13
7.2.1 - Papéis e Responsabilidades.....	13
7.2.2 - Detalhamento	14
8 – SANÇÕES E PUNIÇÕES.....	17
9 – REVISÕES	18
10 – VIGÊNCIA E INSTRUMENTALIZAÇÃO	18

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 3 de 18	Revisão: 03	Publicação: 09/2021


Responsável:	Emilson Queiroz (Gerente TI e Cloud)
Aprovado por:	Suleiman Bragança (CEO)
Políticas Relacionadas:	Política da Segurança da Informação, Código de Conduta e Normas e Procedimentos da Vector Informática
Localização de Armazenamento:	Escritórios de Barueri (SP) / Cuiabá (MT) e Florianópolis (SC)
Data de Aprovação:	11/2021
Data de Revisão:	04/2023
Versão atual:	3.0

1 – INTRODUÇÃO

Essa Política da Gestão de Identidade e Controle de Acesso, complementa a Política Geral de Segurança da Informação, definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação da Vector garanta níveis adequados de proteção.

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Vector, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida. Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos. Os controles de autorização, identificação e

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 4 de 18	Revisão: 03	Publicação: 09/2021

autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação da Vector.

2 - OBJETIVO

Esse documento define as regras de segurança a serem observadas para regulamentar a gestão de usuários, sua identificação e acesso ao sistema da Vector.

3 - ABRANGÊNCIA


Esta política aplica aos colaboradores das Vector, incluindo diretores, empregados, contratados, prestadores de serviço e estagiários, além de quaisquer parceiros de negócio, fornecedores, empresas prestadoras de serviço e colaboradores de parceiros comerciais, com acesso restrito ou acesso autenticado.

4 - REFERÊNCIAS

- Código de Conduta e Ética da Vector Informática;
- Política da Segurança da Informação;


5 - DEFINIÇÕES

- Acesso – Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação da Vector;
- Área Segura – A Vector como utiliza os servidores em Nuvem, então todas suas informações estão restritas nesse ambiente seguro que conta com certificações de provedores de Nuvem (Cloud) com certificações de nível global;
- Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 5 de 18	Revisão: 03	Publicação: 09/2021

utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

- Bloqueio de Acesso – Processo que tem por finalidade suspender temporariamente o acesso;
- Contas de Serviço – Contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script etc.) sem qualquer intervenção humana no seu uso;
- Credenciamento de Acesso – Processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia;
- Credenciais ou Contas de Acesso – Identificações concedidas por autoridade competente após o processo de credenciamento de acesso, que permitam habilitar determinada pessoa, sistema ou conta de um interesse próprio, um Administrador ou Colaborador pode ser influenciado a agir contra os princípios ou interesses da empresa, tomando uma decisão inapropriada ou deixando de cumprir alguma de suas responsabilidades profissionais; organização ao acesso. A credencial pode ser física como crachá, cartão, credencial biométrica ou lógica como identificação de usuário e senha;
- Equipamentos - Instrumentos necessários para determinada função;
- Exclusão de Direito de Acesso – Processo que tem por finalidade suspender definitivamente o acesso;
- Exclusão de Conta de Acesso – Processo que tem por finalidade o cancelamento do código de identificação e do perfil de acesso;
- Gestão de Riscos de Segurança da Informação e Comunicações – Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;


	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 6 de 18	Revisão: 03	Publicação: 09/2021

- Gestor do ativo de informação – indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;
- Identificação do Usuário ou Nome do Usuário – forma pela qual o usuário é conhecido no ambiente de informática da Vector. O usuário recebe as permissões de utilização dos recursos computacionais em função de sua Identificação, que deve ser validada com o uso de uma Senha;
- Perfil de Acesso – Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- Quebra de Segurança – Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;
- Tratamento da Informação – Recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
- Usuário – Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da Vector.

6 – PRINCÍPIOS

O controle de acesso lógico a ativos de tecnologia da informação no âmbito da Vector deve atender aos princípios a seguir:

- Privacidade: Respeitar a privacidade dos usuários e a finalidade de tratamento dos dados pessoais;
- Confidencialidade: Garantir que somente o usuário autorizado possa acessar o ativo de informação;
- Segurança: Prevenir os riscos de acessos indesejáveis e vazamento de informações tratadas pela Vector;
- Autenticidade: Garantir que usuários anônimos acessem somente os ativos de tecnologia da informação considerados públicos;

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 7 de 18	Revisão: 03	Publicação: 09/2021

- Interoperabilidade e otimização de recursos: Usar tecnologias ou processos que atendam o maior número de ativos de tecnologia da informação, quando for viável;
- Não repúdio: Acurácia e precisão na identificação das atividades do usuário.

7 – DESCRIÇÃO


7.1 – CONTROLE DE ACESSO LÓGICO

Conjunto de procedimentos, recursos e meios utilizados pela Empresa com a finalidade de conceder ou bloquear o acesso aos ativos de informação a usuários autorizados ou não.

7.1.1- Papéis e Responsabilidades

1. Tecnologia da Informação (TI):

- Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de empregados, terceiros/prestadores de serviços;
- Conceder, quando autorizado, o acesso aos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Revogar, quando solicitado, o acesso dos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de empregados, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 8 de 18	Revisão: 03	Publicação: 09/2021

2. Gestores:


- Autorizar o acesso às informações sob sua gestão somente para o pessoal baseado estritamente nas necessidades de conhecimento;
- Solicitar a equipe da TI a concessão de acesso novos empregados ou empregados que necessitem de novos acessos conforme mudanças em suas atividades laborais;
- Solicitar a equipe da TI concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;
- Informar a equipe de tecnologia da informação quando ao encerramento do contrato com terceiros/prestadores de serviços contratados que tenham a ativos/sistemas de informação.

3. Departamento Pessoal:

- Reportar em tempo hábil o desligamento de empregados da Vector a equipe de tecnologia da informação para que contas de acesso possam ser revogadas;
- Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na Vector;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

4. Usuários:

- Zelar pela integridade e confidencialidade de suas credenciais de acesso aos recursos computacionais da Vector (identificação de usuário e senha);
- Zelar e contribuir para um efetivo controle de acesso aos recursos computacionais da Vector, de forma a prevenir o acesso não autorizado aos ativos informacionais e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação;
- Assegurar a segurança da informação ao utilizar computação móvel e demais recursos de trabalho remoto.

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 9 de 18	Revisão: 03	Publicação: 09/2021

7.1.2- Detalhamento

1. Criação ou Bloqueio de Conta de Acesso:

- A solicitação para criação ou bloqueio de contas de acessos de usuários, quando do início ou término da prestação de serviço, pode ser realizada pelas áreas do quadro abaixo. A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento de acesso para qualquer usuário.

Área Responsável pela Solicitação de Criação ou Bloqueio de Conta de Acesso	Categorias de Usuário Para os Quais Pode Solicitar a Criação ou Bloqueio de Conta de Acesso
RH	Todos os colaboradores
Gestores	Todos os colaboradores e ou prestadores de serviços

2. Exclusão de Conta de Acesso:


- A exclusão de conta de acesso de um usuário somente poderá ser executada caso sua identificação não tenha sido criada corretamente e não existam registros de logs gerados pelos acessos aos ativos de informação da Vector. Caso tenha ocorrido pelo menos um registro de acesso aos ativos de informação, a conta de acesso deve ser bloqueada indefinidamente.

3. Análise Crítica do Direito de Acesso:

- Cabe ao Gestor da Informação realizar a cada 6 (seis) meses uma análise crítica dos direitos de acesso do usuário aos ativos de informação sob sua gestão. Nos casos de ativos de informações sigilosos, esta análise deve ser feita a cada 3 (três) meses.

4. Integridade e Confidencialidade das Credenciais de Acesso:

- A fim de zelar pela integridade e confidencialidade de suas credenciais de acesso e efetivamente contribuir para a efetiva gestão do controle de acesso aos recursos

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 10 de 18	Revisão: 03	Publicação: 09/2021


computacionais e informacionais da Vector, o Usuário deve seguir as seguintes regras: a) manter a confidencialidade de sua senha pessoal; b) trocar de senha na primeira vez que utilizar a conta de acesso aos sistemas; c) solicitar uma nova senha, quando do esquecimento; d) Evitar o registro das senhas em qualquer meio; e) Alterar a senha sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade.

5. Acesso e Utilização de Computação Móvel:

- Para viabilizar a segurança da informação ao acessar e utilizar computação móvel e demais recursos de trabalho remoto, o usuário deve: a) efetuar o acesso remoto às informações do negócio, pela internet, utilizando-se dos recursos de computação móvel da Vector, após o processo de identificação e autenticação bem-sucedido e com os mecanismos de controle de acesso apropriados; b) evitar ao máximo o acesso à rede de comunicação da Vector a partir de equipamento de terceiros; c) levar em conta a ameaça de acesso não autorizado à informação, ou aos recursos informacionais sob sua responsabilidade, por outras pessoas na residência ou local de trabalho remoto; d) efetuar o processo correto de desconexão quando conectado a partir de um computador remoto.

6. Estações de Trabalho e Outros Ativos de Informação:


- A implementação de um processo de controle de acesso para gerenciar as permissões de acesso a todas as estações de trabalho e outros ativos de informação utilizados na Empresa, não importando sua localização física, deve contemplar os seguintes requisitos gerais: a) possibilitar o gerenciamento do direito de acesso aos diversos ativos de informação; b) conceder os direitos de uso exclusivamente conforme a necessidade; c) estabelecer e manter um processo de autorização e registro de todos os direitos de acesso concedidos; d) contemplar o treinamento dos usuários quanto às boas práticas de segurança na seleção e uso de senhas; e) fornecer um identificador único (conta de acesso) para cada usuário da rede de computadores da Empresa, de forma que cada usuário possa ser identificado e feito responsável por suas ações; f) garantir que as senhas dos usuários dos

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 11 de 18	Revisão: 03	Publicação: 09/2021

recursos computacionais da Vector, quando digitadas, não sejam mostradas na tela de seus respectivos computadores; g) entregar ao usuário, obtendo sua ciência, Termo de Responsabilidade por Ativos de Informação descrevendo seus deveres e obrigações de acesso aos ativos de informação da Vector; h) permitir o acesso somente com os procedimentos de autorização concluídos; i) garantir que o acesso a qualquer recurso computacional esteja sujeito a um processo formal de autorização; j) atualizar o direito de acesso de usuários que tenham mudado de função ou bloquear o direito de acesso de usuários que tenham cessado o vínculo com a Vector; k) estabelecer procedimentos para a proteção dos ativos de informação contra software malicioso; l) prever a realização de auditoria e monitoração da segurança; m) prever a preservação de log de acesso e de tentativas mal sucedidas de acesso aos ativos de informação; n) garantir que a necessidade de bloqueio de acesso do terminal de computador, por inatividade, seja compatível com os riscos de segurança da área e os riscos relacionados aos usuários do terminal; o) garantir que a necessidade de desconexão aos sistemas web, por inatividade, seja compatível com os riscos de segurança da área, a classificação da informação que está sendo manuseada e as aplicações que estão sendo utilizadas.

7. Controle e Autenticação do Acesso Remoto:

- Com a finalidade de prover o controle e a autenticação do acesso remoto pelo usuário, e viabilizar a segurança da informação, quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto, é necessário: a) determinar o nível de proteção e o método de autenticação requerido somente após uma avaliação de risco; b) prover recursos de criptografia para o acesso remoto do usuário; c) estabelecer proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nos recursos móveis; d) criar e manter proteção adequada contra perda, furto ou roubo de informações; caso uma dessas situações ocorra, deve ser possível executar a recuperação rápida e fácil das informações; e) efetuar treinamento especialmente direcionado à segurança e utilização de equipamentos móveis, aos respectivos usuários; f)

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 12 de 18	Revisão: 03	Publicação: 09/2021


permitir o acesso remoto aos recursos computacionais da rede da Vector somente após autorização do Gestor do usuário solicitante; g) provisionar equipamento de comunicação apropriado que inclua métodos seguros de acesso remoto; h) revogar os direitos de acesso remoto quando cessarem as atividades de trabalho remoto; i) proteger computadores e sistemas de comunicação que estejam instalados com recursos que permitem o diagnóstico remoto para manutenção e verificar a real necessidade de interligação ou compartilhamento de recursos de rede e de processamento de informações entre parceiros de negócios; j) implementar um sistema de autenticação dos equipamentos que podem ter acesso às facilidades de comunicação de rede.

8. Utilização de Programas Utilitários:

- Com o objetivo de prover a segurança da informação, quando da utilização de programas utilitários que sejam capazes de sobrepor os controles dos sistemas e aplicações, deve-se: a) utilizar procedimentos de autenticação para utilitários de sistema; b) limitar a utilização dos utilitários de sistemas a um número mínimo de usuários confiáveis e autorizados; c) efetuar o registro de cada uso dos utilitários de sistema; d) definir e documentar todos os níveis de autorização necessários para os utilitários de sistema; e) remover todos os softwares utilitários e demais sistemas desnecessários.

9. Restrição de Acesso do Negócio:

- A fim de assegurar que o acesso à informação e às funções dos sistemas de aplicação, por parte dos usuários, seja baseado nos requisitos de restrição de acesso do negócio e dos respectivos sistemas e serviços, os sistemas aplicativos devem contemplar as seguintes regras: a) fornecer menus para controlar o acesso às funções dos sistemas de aplicação; b) restringir o conhecimento de informações ou funções da aplicação às quais o usuário não tem autorização de acesso, por meio da elaboração de manuais de utilização de sistemas de aplicação direcionados às necessidades do usuário; c) controlar os direitos dos usuários de leitura, escrita, deleção e execução; d) assegurar que as saídas dos sistemas de

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 13 de 18	Revisão: 03	Publicação: 09/2021

aplicação que tratam informações sensíveis contenham somente informações relevantes a essas saídas e sejam enviadas para terminais e locais autorizados.

7.2 – SEGURANÇA FÍSICA

Dispõe sobre a importância da prevenção contra o acesso físico não autorizado que pode causar danos e interferências com as instalações e informações da Vector.

7.2.1 - Papéis e Responsabilidades

1. Gestores:


- Prevenir o acesso não autorizado, dano ou interferência às instalações físicas da Vector;
- Proteger as áreas e perímetros de segurança internos por controles de entrada apropriados;
- Zelar pela segurança patrimonial da empresa, particularmente quando da presença de terceiros nas dependências da Empresa.

2. Tecnologia da Informação – TI:

- Prover o suporte na implementação das regras de segurança física;
- Monitorar continuamente a eficiência e efetividade das medidas de segurança física que afetam a empresa.

3. Usuários:

- Utilizar credencial de acesso físico ostensivo (crachá) em local visível quando nas dependências da Vector;
- Zelar pela proteção e preservação das instalações físicas da Vector.

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 14 de 18	Revisão: 03	Publicação: 09/2021

7.2.2 - Detalhamento

1. Acesso as Instalações


- Ao adentrar as instalações da empresa e durante todo o tempo em que nela permanecer, o empregado da Vector, pessoal terceirizado ou outro colaborador conveniado deve portar sua credencial de acesso (crachá) em local visível;
- Os visitantes devem ser identificados nas áreas de recepção e devem receber um selo de identificação para ser colocado em local visível;
- Os empregados da Vector devem interpelar qualquer pessoa estranha que não esteja acompanhada e qualquer pessoa que não esteja usando uma identificação visível para saber se a mesma está perdida, encaminhando-a à área de recepção mais próxima. A fim de prevenir o acesso não autorizado, dano ou interferência às informações e instalações físicas da Vector.

2. Realização de Trabalhos em Áreas Seguras

- Com a finalidade de assegurar a Segurança da Informação, por ocasião da realização de trabalhos em áreas seguras, as seguintes medidas devem ser observadas: a) divulgar a existência de uma área segura e das atividades nela executadas só quando for realmente necessário. Utilizar controles de acesso para o pessoal ou para terceiros que trabalham dentro da área segura; b) evitar o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para não dar oportunidade a atividades mal-intencionadas; c) permitir atividades de terceiros somente quando autorizado e a atividade possa ser monitorada por empregado do quadro próprio da Empresa; d) trancar e inspecionar periodicamente as áreas seguras desocupadas.

3. Segurança Física dos Equipamentos:

- Para assegurar a proteção dos equipamentos, é necessário: a) proteger os equipamentos fisicamente contra as ameaças à sua segurança e dos perigos ambientais; b) planejar a localização e disposição dos equipamentos, de modo a reduzir o risco das ameaças e perigos do meio-ambiente e as oportunidades de

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 15 de 18	Revisão: 03	Publicação: 09/2021


acesso não autorizado; c) adotar controles para minimizar o risco de ameaças potenciais, incluindo furto, incêndio, fumaça, água (ou falha no abastecimento), poeira, vibração, efeitos químicos, interferência no suprimento de força e radiação eletromagnética; d) proibir comer, beber e fumar nas instalações de processamento de informações ou em sua proximidade; e) monitorar as condições ambientais quanto a fatores que podem afetar negativamente a operação dos equipamentos de processamento de informações; f) considerar o impacto de um acidente em instalações próximas, como por exemplo, um incêndio no prédio vizinho ou em outras empresas localizadas no mesmo prédio, vazamento de água do telhado, ou dos andares acima da Vector, ou uma explosão na rua; g) proibir a identificação dos equipamentos de processamento de informações sensíveis nas listas de pessoal e listas telefônicas internas ou em locais acessíveis ao público.

4. Proteção de Informações e de Recursos de Processamento:

- Visando evitar exposição ou roubo de informações e de recursos de processamento da informação das salas e instalações, deve-se: a) adotar procedimentos para garantir a política de mesa limpa e tela limpa; b) posicionar equipamentos críticos em local não acessível ao público; c) posicionar funções e equipamentos de suporte, equipamentos como fotocopiadoras e fax, num local apropriado dentro da área segura; d) implantar sistemas apropriados de detecção de intrusos, instalados segundo padrões profissionais, e testados regularmente para cobrir todas as portas externas; e) dispor alarme armado permanentemente nas áreas não ocupadas; f) dispor equipamentos administrados pela organização fisicamente separados dos equipamentos administrados por terceiros; g) posicionar a uma distância segura os equipamentos e mídia de backup, para que não sejam danificados em caso de um acidente no site principal da organização.

5. Suprimento de Energia Elétrica e Água:

- A fim de garantir o suprimento adequado de eletricidade que atenda às especificações dos fabricantes dos equipamentos, evitando-se quedas e oscilações de tensão frequentes e sobrecargas, deve-se: a) manter plantas atualizadas da rede

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 16 de 18	Revisão: 03	Publicação: 09/2021


elétrica; b) utilizar múltiplas fontes de alimentação para evitar que o suprimento dependa de uma única fonte, sempre que possível; c) fornecer suprimento de energia à prova de interrupções (sistema no break) para os equipamentos dos CPDs e para os ativos críticos e/ou sensíveis.

6. Utilização de Equipamentos Fora das Instalações:

- Quanto à segurança dos equipamentos fora das instalações da Vector, deve-se: a) adotar procedimentos de segurança para todo ativo (todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, papel ou outros meios) que ficam na posse da pessoa para trabalho a domicílio ou que são transportados para fora do local normal de trabalho.

7. Segurança no Descarte ou na Reutilização de Equipamentos e Materiais:

- No descarte ou na reutilização de equipamentos e materiais que contenham qualquer tipo de informação, deve-se atentar aos cuidados necessários conforme o tipo de equipamento e material e a informação neles contidos;
- Deve-se destruir fisicamente ou sobrescrever de maneira segura (ao invés de se usar a função delete) os sistemas de armazenagem que contenham informações sensíveis;
- Devem-se verificar todos os itens de equipamento que contenham mídia de armazenagem, como por exemplo, discos rígidos, para garantir que todos os dados sensíveis e softwares licenciados tenham sido retirados ou sobrescritos antes do descarte ou reutilização;
- Os dispositivos de armazenagem danificados devem ser avaliados quanto às informações neles contidos, para determinar a conveniência de serem consertados, descartados ou destruídos;
- Os materiais que contenham informações (CDs, papel etc..) devem ser destruídos de forma a impedir sua recomposição.

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 17 de 18	Revisão: 03	Publicação: 09/2021

8. Equipamentos de Prevenção e Combate a Incêndios:


- Quanto aos equipamentos de prevenção e combate a incêndios, produtos e locais críticos, deve-se: a) manter a compatibilidade dos equipamentos de prevenção e combate a incêndios com o ambiente onde podem vir a ser necessários.

9. Condições Gerais de Segurança da Edificação:

- A fim de zelar pela segurança da edificação, deve-se: a) remover o lixo diariamente; b) verificar periodicamente a necessidade de efetuar dedetização e desratização; c) proibir a execução de trabalho que gerem poeira na área dos equipamentos, sem que sejam tomados os cuidados necessários para a execução dos mesmos; d) manter trancados os quadros de conexões telefônicas e distribuição do cabeamento de rede e garantir que o acesso somente seja permitido ao pessoal autorizado; e) manter e testar os detectores de fumaça de forma programada; f) instalar sensores de temperatura e umidade do ar; g) verificar a necessidade de suplementar os recursos condominiais com quadros de controle que detectem e localizem rapidamente fogo e fumaça; h) manter plantas de localização dos extintores e detectores; i) manter sensoramento de portas, janelas, dutos e supervisão predial; j) verificar as saídas de emergência em relação à usabilidade periodicamente; k) manter uma rede de iluminação bem distribuída e de boa qualidade com iluminação de emergência; l) fornecer manual ao corpo de vigilantes ou agentes prediais com procedimentos de emergência; m) dispor de quadros de luz e iluminação em locais adequados; n) manter o controle da temperatura.

8 – SANÇÕES E PUNIÇÕES

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação e na Política da Gestão das Consequências.

	COMPLEMENTO DA PSI - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Última Revisão – 04/2024		
		Página 18 de 18	Revisão: 03	Publicação: 09/2021

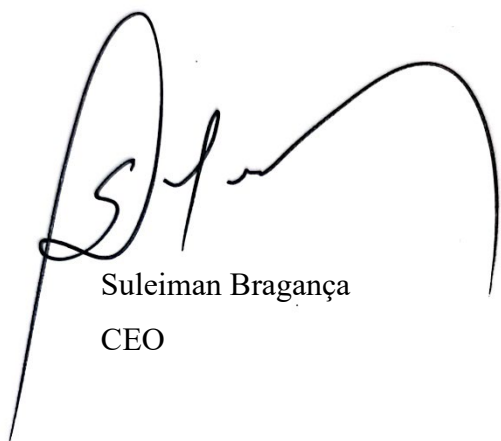
9 – REVISÕES

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê de Segurança da Informação.

10 – VIGÊNCIA E INSTRUMENTALIZAÇÃO

A presente Política de Gestão de Identidade e Controle de Acesso da Vector tem vigência a partir de sua data de publicação e validade indeterminada, e ser decidido pela Diretoria e pelo Comitê de Segurança da Informação, e posteriormente divulgado a todos os interessados.

Barueri, novembro de 2021



Suleiman Bragança
CEO