





**POLÍTICA COMPLEMENTAR DA
SEGURANÇA DA INFORMAÇÃO /
CIBERNÉTICA**

NOVEMBRO - 2021


	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 2 de 37	Revisão: 03	Publicação: 11/2021

Sumário

1 – INTRODUÇÃO.....	4
2 - PRINCÍPIOS.....	5
3 - OBJETIVOS	6
4 - ABRANGÊNCIA.....	6
5 – TESTE DE PENETRAÇÃO, VULNERABILIDADE E MONITORAMENTO	7
6 – ATUALIZAÇÕES E GERENCIAMENTO DE PATCHES.....	8
7 – PENTESTS.....	9
8 – HARDENING DAS ESTAÇÕES DE TRABALHO	10
9 – CONTROLES DE LOGS.....	11
9.1 – Composição e Retenção dos Registros de Eventos na Rede e nos Sistemas.....	11
9.2 – Tempo de Retenção dos Eventos de Acesso ou Uso.....	12
9.3 – Monitoramento dos Eventos de Acesso ou Uso.....	12
9.4 – Monitoramento dos Eventos de Incidentes ou Falha.....	14
9.5 – Da Proteção das Informações dos Registros de Eventos.....	14
9.6 – Dos Registros de Eventos de Administrador e Operador.....	15
9.7 – Da Sincronização dos Relógios.....	15
10 – FIREWALL.....	16
11 – CRIPTOGRAFIA.....	17
12 – DESENVOLVIMENTO SEGURO.....	19
12.1 – Armazenamento de Dados.....	19
12.2 – Gerenciamento e Distribuição de Senhas para Acesso a Dados.....	20
12.3 – Comunicação Segura	21
12.4 – Ataques á Sistemas e suas Defesas.....	21
12.5 – Auditoria, Rastreamento e LOGS.....	22
12.6 – Prevenção, Reação e Mitigação de Falhas de Segurança.....	23

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 3 de 37	Revisão: 03	Publicação: 11/2021

12.7 – Ambiente de Desenvolvimento	25
12.8 – Proteção de Dados	26
12.9 – Ciclo de Vida de Software.....	27
13 – GESTÃO DE INCIDENTES DE SEGURANÇA.....	28
13.1 – Monitoramento e Gerenciamento de Incidentes.....	31
13.2 – Plano de Resposta a Incidentes e Informações Acerca da Segurança Cibernética	32
14 – RESPONSÁVEIS A SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	34
14.1 - Responsável pela Segurança da Informação / Cibernética.....	34
14.2 – Comitê de Segurança da Informação / Cibernética	35
14.3 – Demais Atribuições – Todos Colaboradores	36
15 - CONSIDERAÇÕES FINAIS.....	37

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 4 de 37	Revisão: 03	Publicação: 11/2021

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:	04/2024
Versão atual:	3.0


1 – INTRODUÇÃO

Para complementar as normas sobre a gestão da Segurança da Informação, foi realizado pela TI da Vector essa Política Complementar da Segurança da Informação / Cibernética

A presente Política de Ciber-Segurança visa a estabelecer princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Vector Informática Ltda., assegurando a proteção adequada dos ativos e dos dados tratados por ela, garantindo, assim, a identificação, proteção, detecção, resposta e recuperação de contingências em casos de eventuais incidentes de segurança.

A Vector busca atingir um alto padrão de cibersegurança. Por isso, está comprometida com a segurança de todos os ativos físicos e lógicos de informação da empresa, garantindo que todos os requisitos legais, operacionais e contratuais sejam cumpridos.

A preocupação com os riscos cibernéticos é comum aos diversos níveis de gestão e um compromisso individual de todos. Nesse sentido, de modo a cumprir com os valores da Vector, a presente Política tem como premissa:


	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 5 de 37	Revisão: 03	Publicação: 11/2021

- Estabelecer diretrizes de cibersegurança, visando a proteger os ativos de tecnologia e os dados dos clientes da Vector;
- Informar os Colaboradores da Vector e atribuir responsabilidades para garantia da segurança da informação, prevista em política própria; e
- Garantir o cumprimento dos mais elevados padrões de ética e integridade, bem como de leis, normas, regulamentos, códigos, diretrizes e padrões aplicáveis aos negócios da Vector.

2 - PRINCÍPIOS

A Vector adotará os seguintes atributos básicos de cibersegurança em conformidade com os padrões internacionais:

- **Confidencialidade:** a Vector limitará o acesso à informação tão somente às entidades legítimas, ou seja, àquelas pessoas autorizadas pelo proprietário da informação;
- **Integridade:** todas as informações manipuladas pela Vector manterão todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida;
- **Disponibilidade:** atributo que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pela Vector;
- **Autenticidade:** a Vector garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;
- **Irretratabilidade ou não repúdio:** propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;
- **Conformidade:** a Vector seguirá as leis e regulamentos associados ao processo de segurança das informações.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 6 de 37	Revisão: 03	Publicação: 11/2021

3 - OBJETIVOS

Entre os objetivos desta Política estão:


- Proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados;
- Assegurar a continuidade do processamento das informações críticas ao negócio;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Determinar os mecanismos de gestão de riscos cibernéticos; e
- Dar ciência ao público em geral.

4 - ABRANGÊNCIA

Esta Política estabelece princípios que devem nortear condutas e regras a serem observadas por todos os sócios, diretores, administradores, empregados, estagiários e, ainda, fornecedores e prestadores de serviços (“Colaboradores”) que venham, direta ou indiretamente, trabalhar ou prestar serviços para a Vector.

As premissas definidas nesta Política são aplicáveis a todos os ambientes computacionais de processamento de dados da Vector, estendendo, sem limitação, a todos os servidores, bases de dados, sistemas operacionais, hardware, software, dispositivos de redes, telefonia, dispositivos móveis, além de ambientes de terceiros que, de forma física ou lógica, estejam integrados ou conectados aos ambientes da Vector e seu acervo tecnológico.

Assim, toda a atividade desempenha pela Vector deve respeitar os princípios estabelecidos nesta Política, devendo tais princípios serem aplicados a todos os que estão acima mencionados. Adicionalmente, todos deverão zelar pela lealdade, honestidade, transparência e o respeito mútuo nas relações profissionais e pessoais com clientes, potenciais clientes, concorrência, fornecedores, órgãos reguladores e fiscalizadores, prestadores de serviços e entre si. Fica, portanto, vedado aos Colaboradores

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 7 de 37	Revisão: 03	Publicação: 11/2021

descumprirem as regras desta Política ou qualquer lei, regra ou regulamentação da legislação aplicável ao tema.


5 – TESTE DE PENETRAÇÃO, VULNERABILIDADE E MONITORAMENTO

A Gestão de Vulnerabilidades refere-se ao risco dos dados da Vector e de seus clientes, armazenados em plataformas tecnológicas, serem comprometidos, roubados e/ou divulgados a uma parte não autorizada. Além dos procedimentos e controles adotados previstos nesta política, para mitigar este risco, a TI da Vector deve implementar e monitorar processos para a identificação proativa de vulnerabilidades técnicas, priorização da correção de vulnerabilidades identificadas usando uma abordagem baseada em risco e resolução oportuna de vulnerabilidades por meio de aplicação de patches de segurança ou implementação de outros controles de compensação apropriados.

Serão realizados testes de penetração e vulnerabilidade na infraestrutura tecnológica da Vector afim de verificar possíveis problemas de segurança e corrigi-los preventivamente. Esses testes serão realizados por empresas independentes, especializadas em segurança e escolhidas a critério da Vector, hoje a Vector utiliza o Fornecedor AWS.

Tais testes serão realizados pelo menos uma vez ao ano ou sempre que houver mudança significativa na infraestrutura utilizada pela Vector ou seus parceiros. O prazo para correção dos problemas encontrados poderá variar dependendo da classificação de severidade dos mesmos, entretanto a Vector envidará todos os esforços necessários para que as correções sejam realizadas no menor tempo possível, a saber: Severidade Prazo
Baixa 120 dias Média 90 dias Alta 60 dias Crítica Imediata ou o mais breve possível

Uma vez identificada alguma vulnerabilidade, seja nos ativos e serviços de tecnologia (internos e externos), a Vector deve registrar onde ocorre, identificar os riscos diretos e indiretos, definir plano de ação, nível de classificação e respectivo prazo para correção e indicar um responsável pela gestão da vulnerabilidade. O responsável pela gestão, assim

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 8 de 37	Revisão: 03	Publicação: 11/2021

como a TI da Vector devem efetuar o monitoramento da adequação quanto ao nível de controle e cumprimento desta Política, assim como do Manual de Segurança da Informação.


Hoje na Vector não é necessário fazer testes de vulnerabilidade porque todos os dados corporativos, estão em ambiente hermético de nuvem, como não existe nenhum dado corporativo salvo nas premissas da empresa, bem como em qualquer dispositivo de trabalho, ademais a necessidade da maioria dos colaboradores executarem seus trabalhos de forma home office devido a pandemia, a Vector se vale de garantir atualizações de segurança das workstations bem como do software anti ameaças digitais e mantendo canal seguro sem troca de dados entre a workstation e os sistemas na nuvem via Área de Trabalho Remoto com VPN. Segurança na Nuvem garante uma qualidade de segurança superior do que se for a local.

Como nosso Fornecedor de serviços em Rede Cloud já executa os aplicativos de Segurança automaticamente. Um dos aplicativo que nosso fornecedor utilizar para monitorar e rastrear a segurança é o: Configure Windows Updates - esse aplicativo é usado por muitos recursos de segurança do Windows para fornecer notificações sobre a integridade e a segurança do computador. Isso inclui as notificações sobre firewalls, produtos antivírus, Windows Defender SmartScreen e outros.

Então o papel hoje, e acompanhar os relatórios dos testes realizados pelo nosso Fornecedor de serviços em Rede Cloud – AWS.

6 – ATUALIZAÇÕES E GERENCIAMENTO DE PATCHES

A Vector mantém os sistemas operacionais e softwares de aplicação sempre modernizados, instalando as atualizações sempre que forem aplicáveis. Os patches disponíveis são gerenciados de modo a permitir o controle sobre o que deve ou não ser atualizado com o fim de rastrear e implementar melhorias necessárias, corrigindo

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 9 de 37	Revisão: 03	Publicação: 11/2021

vulnerabilidades identificadas na estrutura tecnológica para o caso de riscos classificados como críticos, médios ou altos.


Os servidores de produção e contingência possuem processo automático para verificação dos últimos patches disponibilizados pelo fornecedor e dispara e-mail automático a Equipe de Tecnologia informando semanalmente a necessidade da aplicação dos patches.

Os produtos são contratados As a Service (ad, file server, banco de dados, web server, balanceadores, firewall, etc), esta atualização é feita automaticamente pelo fornecedor de serviço, no caso AWS.

Nos desktops é reforçado por ferramenta de gerenciamento forçando atualização semanal.

7 – PENTESTS

- A execução de Testes de Penetração deve ser realizada no mínimo duas vezes ao ano ou quando houver uma mudança significativa do ambiente. O processo deve ser realizado por uma empresa terceira de comprovada idoneidade, que tenham profissionais comprovadamente capacitados;
- Os testes de penetração devem comprovar a eficácia dos controles de segmentação;
- Ao fim do Teste de Penetração deve ser gerado um relatório identificando o que foi feito, como foi feito, quando foi feito, vulnerabilidades, evidências e sugestões de remediação;
- O escopo do Teste de Penetração deve ser todos os ativos (servidores, sites etc.);
- O Teste de Penetração deve seguir metodologias reconhecidas internacionalmente pela área de segurança da informação;
- O Teste de Penetração feito pela própria equipe poderá ser realizado periodicamente desde que se tenha alguém capacitado para fazer e com a devida aprovação da empresa;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 10 de 37	Revisão: 03	Publicação: 11/2021

- O Teste de Penetração feito pela própria empresa não substitui a contratação de um terceiro para realizar o procedimento ao menos 2 vezes ao ano;
- Todas as vulnerabilidades encontradas no Teste de Penetração que forem exploráveis devem ser analisadas e corrigidas imediatamente;
- Após promovidas as correções, deve-se realizar novos testes com a finalidade de comprovar a efetividade das correções;
- As correções efetuadas baseadas no relatório de Teste de Penetração devem ser documentadas e guardada.


Conforme descrito acima será esses requisitos para fazer os Pentests na Vector. Mas hoje a Vector como não possui infraestrutura de servidores, somente servidores em nuvem, ela utiliza os serviços do Fornecedor AWS para executar seus Pentests.

Além disso, e acordado com a AWS deve ter a premissa de documentar explicitamente que o provedor de serviços notifique a Vector de forma tempestiva caso haja algum tipo de violação no serviço, independente das partes ou dados envolvidos.

8 – HARDENING DAS ESTAÇÕES DE TRABALHO

A Vector utiliza a técnica de blindagem (Hardening) em todas as suas estações de trabalho. Usando essa técnica para mapear as ameaças, mitigação dos riscos e execução das atividades corretivas. Com o objetivo de deixar a rede da Vector mais segura para enfrentar tentativas de ataques e invasões. Exemplo dessas regras:

- Praticar toda a nossa política de segurança;
- Desabilitar e/ou deletar contas desnecessárias, portas e serviços em nossas estações de trabalho;
- Desinstalar aplicações não necessárias;
- Configurar o firewall do Windows;
- Desabilitar compartilhamentos desnecessários;
- Configurar a encriptação;
- Atualizando e aplicando patches de segurança;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 11 de 37	Revisão: 03	Publicação: 11/2021

- Uso de Antivírus e NAP;
- Controle total dos acessos a rede VPN.

Como a Vector não salva dados corporativos, é utilizado as boas práticas de mercado e mecanismo de proteção contra ameaças digitais.

Para ambiente de Data Center a Vector utiliza de toda camada de proteção e certificados do provedor de serviço.

De forma geral seguimos boas práticas de mercado como POLP, Segregação de Função, etc, Ou seja, Nos beneficiamos das certificações de provedor de nuvem de nível global. Além de prioriza a contratação de CaaS, PaaS, DBaaS e SaaS de provedor de renome global, onde o mesmo garante a continuidade do serviço, liberando a empresa para a Arquitetura e Gestão do ambiente. E também categorizamos-nos como depositários dos dados do cliente, onde o mesmo define as compliances, sendo os acessos aos dados feito apenas a nível de serviço.

9 – CONTROLES DE LOGS


Estas diretrizes sobre controles de Logs é um complemento da Política de Identidade e Controle e Acesso da Vector.

Essas diretrizes desse documento sobre controle e monitoramento de Logs é mais voltado para a equipe de Desenvolvimento.

9.1 – Composição e Retenção dos Registros de Eventos na Rede e nos Sistemas

Os registros de eventos devem conter informações mínimas e relevantes, especialmente:

- Identificação inequívoca do usuário que acessou o recurso;
- Identificação dos usuários de origem e destino do evento, quando for o caso;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 12 de 37	Revisão: 03	Publicação: 11/2021

- Natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha, entre outros;
- Timestamp, formado por data, hora e fuso horário;
- Endereço de Internet Protocol (IP), identificador do ativo de processamento, coordenadas geográficas, se disponíveis, e outras informações que permitam identificar a possível origem e destino do evento;
- Endereços, serviços e protocolos de rede utilizados;
- Arquivos acessados e tipo de acesso;
- Alarmes provocados pelo sistema de controle de acesso.

Os ativos de processamento que não permitam os registros de eventos conforme indicado devem ser mapeados e documentados quanto ao tipo e ao formato de registro de eventos que o sistema permite armazenar.


9.2 – Tempo de Retenção dos Eventos de Acesso ou Uso

Os registros de eventos devem ser armazenados na rede Vector, pelo período de 30 (trinta) dias, e em mídias não regraváveis, por um período mínimo de 12 (doze) meses, sem prejuízo de outros prazos previstos em referências legais e normativas específicas.

9.3 – Monitoramento dos Eventos de Acesso ou Uso

Os ativos de processamento em produção devem ser configurados de forma a gerar registros de eventos relevantes que afetem a segurança da informação, armazenando-os para utilização posterior, incluindo:

- Acesso remoto à rede Vector;
- Autenticação, tanto a bem-sucedida quanto a malsucedida;
- Criação, alteração e remoção de usuários, perfis e grupos privilegiados;
- Uso de privilégios;
- Troca de senhas;
- Modificação de política de senhas, como tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras;


	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 13 de 37	Revisão: 03	Publicação: 11/2021

- Acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos;
- Alteração na configuração de sistemas operacionais, serviços e sistemas de informação;
- Inicialização, suspensão e reinicialização de serviços;
- Uso de aplicativos e utilitários do sistema operacional;
- Ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusos;
- Acesso físico por senha, cartão magnético ou biometria em área de segurança com ativos de processamento críticos como data center, entre outros;
- Acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;
- Acesso e alteração nos registros de eventos (logs).

O monitoramento deve ser realizado, preferencialmente, com a utilização de ferramentas automatizadas que gerem alarmes imediatos de eventos críticos e permitam a correlação e análise dos registros de eventos gravados.

1. O monitoramento deve ser realizado de forma a manter inalterada a rotina de trabalho do ambiente de produção.
2. O nível de monitoramento pode ser reduzido em função da implementação de controles de acesso que minimizem o risco aos ativos de processamento e reduzam a exposição da informação a acessos indevidos.
3. As ferramentas automatizadas devem ser analisadas criticamente a intervalos regulares para ajustar sua configuração, de forma a melhorar a identificação de registros de eventos relevantes, falsos negativos e falsos positivos.

Os processos de monitoramento devem ser revisados na implantação ou na manutenção dos ativos de processamento, a fim de manter sua adequação às mudanças ocorridas.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 14 de 37	Revisão: 03	Publicação: 11/2021

Os usuários devem estar cientes de que os ativos de processamento estão suscetíveis a monitoramento e auditoria sempre que houver suspeita ou constatação de quebra de segurança.

9.4 – Monitoramento dos Eventos de Incidentes ou Falha

Todos os eventos contrários a Política de Segurança da Informação do Vector, devem ser registrados formalmente e analisados, com adoção das ações apropriadas para sua correção:


- Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados Vector, terá consequências de acordo com a Política de Consequências da Vector;
- Interrupção de serviço;
- Modificação ou alteração pelo colaborador ou programa de informática sem autorização;
- Interceptação clandestina.

9.5 – Da Proteção das Informações dos Registros de Eventos

Os arquivos de registros de eventos devem ser protegidos para que não sejam possíveis o acesso não autorizado às informações registradas e/ou a falsificação destas.

A fim de assegurar a proteção, os seguintes controles mínimos devem ser implementados:

- Armazenamento, no mínimo, em 2 (dois) arquivos de mesmo conteúdo, sendo um deles em local centralizado e protegido contra acessos indevidos;
- Guarda da cópia centralizada em segmento isolado da rede corporativa, com proteção de dispositivos de segurança, tais como firewall, sistema de detecção e prevenção de intrusões, entre outros;
- Espaço de armazenamento adequado e alertas preventivos de seu esgotamento;
- Localização física em área sujeita a controles de segurança;
- Emprego de protocolos seguros para acesso remoto;
- Capacidade de assinatura digital ou resumo criptográfico para verificar a integridade;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 15 de 37	Revisão: 03	Publicação: 11/2021

- Execução de auditorias legais realizados pelo Comitê de Segurança da Informação da Vector;
- Fornecimento, para efeito de investigação, de cópia das informações relevantes, exceto nas hipóteses legais que exijam a apresentação da mídia original;
- Geração de registros de eventos (logs) para todos os trabalhos executados nos arquivos;
- Conservação de documentação atualizada dos procedimentos de: a) configuração, instalação e manutenção; b) administração e operação; c) cópia de segurança e restauração.

9.6 – Dos Registros de Eventos de Administrador e Operador


Os registros de eventos de administradores e operadores com privilégios para ações e comandos especiais na rede Vector, como superusuários, administradores de rede, entre outros, devem ter mecanismos adicionais de gerenciamento e monitoramento, considerando, no mínimo, os seguintes aspectos:

- Os registros de eventos dos administradores e operadores da rede da Vector devem ser protegidos e analisados criticamente, a intervalos regulares;
- Os administradores e operadores da rede da Vector não devem fazer parte da equipe de monitoramento e análise crítica de suas próprias atividades;
- Os administradores e operadores da rede da Vector não devem ter permissão para apagar, alterar ou desativar os registros de eventos de suas próprias atividades.

Um sistema de detecção e prevenção de intrusões gerenciado fora do controle dos administradores e operadores da rede da Vector pode ser utilizado para monitorar as atividades nos registros de eventos.

9.7 – Da Sincronização dos Relógios

O horário dos ativos de processamento deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 16 de 37	Revisão: 03	Publicação: 11/2021

O estabelecimento correto dos relógios nos ativos de processamento da rede da Vector é importante para assegurar a exatidão dos registros de eventos, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares, devendo atender, no mínimo, às seguintes rotinas:

- Uso de, pelo menos, 3 (três) fontes de tempo sincronizadas, a partir das quais os ativos de processamento recuperem regularmente as informações de data, hora e fuso horário, de forma que os registros de eventos (logs) sejam cronologicamente consistentes;
- Preferencialmente, compartilhamento ou sincronização das mesmas fontes de tempo com outros controles de acesso lógico e físico, como catracas, pontos eletrônicos, entre outros, para integrar cronologicamente os sistemas de gerenciamento.

10 – FIREWALL

A Vector adota firewalls de última geração, que permitem analisar em tempo real a camada em que os softwares estão presentes, protegendo contra ameaças conhecidas e desconhecidas dentro de aplicações.


No que se refere ao processamento, armazenamento de dados e computação em nuvem:

Na Vector, os serviços de processamento, armazenamento de dados e computação em nuvem são oferecidos pela empresa Amazon Web Services (AWS). Utilizamos os produtos nativos do provedor AWS que são:

- AWS Firewaal (Route, NAT, ACL, Security Group);
- AWS WAF (Web Application Firewall);

AWS possuem mecanismos de proteção contra vírus maliciosos. Para toda estrutura de servidores há camada de antivírus.

Os dados sendo trafegados entre a AWS e a Vector são protegidos contra acesso indevido.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 17 de 37	Revisão: 03	Publicação: 11/2021

Para a comunicação entre o fornecedor de Data Center e a Vector, a estrutura de link é formada por Link Lan-to-Lan dedicado e com dupla abordagem de operadoras, onde em toda estrutura possui uma VLAN dedicada para segmentação de seu tráfego até a chegada do firewall.

Adicionalmente, a estrutura de redes e segurança do Data Center é composta por equipamentos redundantes, onde na camada externa, juntamente com os roteadores de borda, há solução de proteção contra ataques DDoS. A camada de firewall é formada por equipamentos que trabalham da Camada 3 à Camada 7 com as devidas regras de liberação ou bloqueio. Juntamente a essa solução, há também os recursos de IPS/IDS e WAF para prevenção de ataques e vazamento de informações por meio de acessos indevidos.

No que se refere à segurança de rede e ao uso de Internet a Vector, deve manter sua rede segmentada e restringir o acesso direto à internet das estações de trabalho e servidores por meio de firewall. O firewall também dispõe de ferramentas que permitem monitorar e registrar a navegação dos usuários a fim de detectar, rastrear e bloquear vazamentos de dados sigilosos;


A área de Segurança da Informação é responsável por controlar as regras de firewall e gerir as demandas de alteração do firewall.

A TI também deve monitorar todos os logs gerados pelo firewall, analisando periodicamente, a fim de identificar possíveis problemas de segurança.

11 – CRIPTOGRAFIA

O uso de chaves de criptografia e certificados digitais são mecanismos de segurança para proteção de dados e ativos sensíveis da Vector, possibilitando a mitigação de riscos, além de cumprir com leis e regulamentações em vigor.

Como forma de proteção, a Vector utiliza criptografia para dificultar a legibilidade dos dados tratados por terceiros não autorizados.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 18 de 37	Revisão: 03	Publicação: 11/2021

A Vector usa a criptografia em todas as senhas de suas aplicações. O sistema transacional dos negócios e de gestão corporativa possui software de versionamento para guarda de código fonte, bem como possui backup tanto do código fonte como também das versões dos instaladores das aplicações.

A Vector investe em treinamento de metodologia em desenvolvimento seguro para seus colaboradores e usa programas para análises SAST e DAST de suas aplicações.

Qualquer acesso externo aos sistemas, seja para cliente, colaborador ou fornecedor, é disponibilizado em canal seguro e criptografado.


Todas as senhas de usuários são armazenadas de forma criptografadas.

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação. Algoritmos criptográficos devem ser aplicados conforme a necessidade em dados em repouso, em trânsito e/ou em uso.

Devem ser assegurados pelas equipes de TI o uso efetivo da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade das informações corporativas.

A chave para descriptografar os dados tratados pela Vector deverão ser mantidos em sigilo, sendo seu acesso permitido apenas aos Colaboradores autorizados, de modo a impedir que qualquer pessoa possa decifrar os dados em trânsito ou em repouso.

No caso de suspeita ou conhecimento de que as chaves de criptografia tenham sido comprometidas, essas deverão ser substituídas o mais breve possível para evitar acessos indevidos ou vazamento de dados sensíveis. Além disso, quando um funcionário com conhecimento das chaves de criptografia encerra suas atividades na Vector, as chaves que eram de conhecimento desse funcionário deverão ser substituídas o mais breve possível.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 19 de 37	Revisão: 03	Publicação: 11/2021

12 – DESENVOLVIMENTO SEGURO

Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações. Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas.

Essa Política apresenta as diretrizes para desenvolvimento seguro de software no âmbito da Vector, seu objetivo é servir como guia de boas práticas a serem adotadas por analistas, desenvolvedores de software, tornando o processo de concepção dos sistemas construídos mais confiáveis, auditáveis, estável e protegido contra ameaças. Essas normas são direcionadas a todos os envolvidos no processo de desenvolvimento de software da Vector.

12.1 – Armazenamento de Dados


Segue as definições e diretrizes que tratam do armazenamento de informações sigilosas ou não, e de sua disponibilização.

1 Procedimentos e Meios para Armazenamento de Dados

- Não se deve utilizar meio de armazenamento que não possua acesso para leitura e escrita restrito por senha.
- Deve-se preferencialmente armazenar dados de forma criptografadas.

2 Permissões para Acesso a Informações em Banco de Dados

- Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões de root.
- Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões para execução de comandos em Data Definition Language (DDL).

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 20 de 37	Revisão: 03	Publicação: 11/2021

- Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões além das estritamente necessárias ao seu funcionamento.

3 Gerenciamento e Distribuição de Senhas para Acesso a Dados

- Não se deve permitir a elaboração de senhas que não sigam os padrões estabelecidos pela Vector.
- Não se deve utilizar o armazenamento de senhas em código-fonte.
- Deve-se armazenar de forma segura os dados de usuários e os sistemas que utilizam cada senha fornecida.
- Não se devem utilizar as mesmas senhas para ambientes de desenvolvimento, teste, homologação e produção.

12.2 – Gerenciamento e Distribuição de Senhas para Acesso a Dados


Esta seção apresenta definições e diretrizes que tratam do controle de acesso aos dados e a atribuição das permissões necessárias.

1. Autorização e Autenticação de Usuários

- Não se deve armazenar senhas em texto plano sem utilizar um algoritmo de hash seguro e salt.
- Deve-se utilizar controle de usuário e senha nominais para determinar a identidade do usuário.
- Deve-se utilizar autenticação via AD sempre que possível para autenticar usuários internos.
- Deve-se dar ciência ao usuário das permissões e níveis de acesso que possui.
- Deve-se utilizar grupos de Active Directory (AD) para determinar as políticas de acesso e roles de usuário.

2. Autenticação em Sistemas Web

- Sendo o HTTP um protocolo stateless, que utiliza cookies para manter sessões de usuário, faz-se necessário garantir tanto a segurança da troca de credenciais

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 21 de 37	Revisão: 03	Publicação: 11/2021

quanto a segurança das demais páginas acessadas pelos usuários dos sistemas web. O protocolo HTTPS visa contribuir para que essa segurança seja garantida.

- Dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas.

12.3 – Comunicação Segura


Esta seção apresenta definições e diretrizes que tratam da transmissão segura de dados sensíveis entre sistemas, de modo a salvaguardar a integridade, autenticidade e demais atributos pertinentes ao uso dos dados comunicados.

- Deve-se empregar canal de comunicação com controle de duplicação e perda de informações/mensagens. Dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas.
- Deve-se empregar canal de comunicação que provenha controle de integridade dos dados transmitidos (HTTPS).
- Deve-se empregar canal de comunicação com controle de autenticação (HTTPS, certificados digitais gerados por autoridades confiáveis, VPNs).
- Deve-se armazenar de maneira segura os dados a serem transmitidos em ambas as extremidades da comunicação.
- Deve-se empregar canal de comunicação que provenha confidencialidade dos dados transmitidos (HTTPS e VPNs).

12.4 – Ataques á Sistemas e suas Defesas

Esta seção apresenta diretrizes para reforçar a resiliência de sistema a ataques contra sistemas e aplicações. Recomenda-se que sejam prevenidos os principais ataques conhecidos, de forma a evitar que ataques mal-intencionados possam comprometer a segurança do sistema, expor dados sigilosos e realizar operações não autorizadas, dentre outras vulnerabilidades.

- Deve-se prevenir ataques de injeção de SQL (SQL Injection).

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 22 de 37	Revisão: 03	Publicação: 11/2021


- Não se deve criar SQLs concatenando parâmetros textuais de origem não-segura, como parâmetros preenchidos pelo usuário ou mesmo armazenados no banco de dados.
- Deve-se restringir permissões de acesso ao banco de dados para o usuário da aplicação.
- Deve-se, sempre que possível, passar parâmetros em comandos SQL (DML ou DDL) utilizando prepared statements. Consultas que não podem ser parametrizadas deverão receber tratamento especial, como escapes ou codificação em hexadecimal.
- Deve-se prevenir ataques de injeção de HTML e Javascript.
- Deve-se prevenir ataques do tipo cross-site scripting (XSS).
- Deve-se prevenir ataques de quebra de autenticação e gerenciamento de sessão (Broken Authentication and Session Management).
- Deve-se submeter os sistemas a ferramentas de testes de invasão.

12.5 – Auditoria, Rastreamento e LOGS

Esta seção apresenta diretrizes para a manutenção de registros/logs para posterior auditoria, rastreamento e consulta de incidentes ligados à segurança dos sistemas. Cada sistema possui uma criticidade diferente no que se refere a restrição de acesso a dados, não-repúdio e histórico de operações realizadas no banco de dados. Por esse motivo, essa seção não define quais informações devem ser auditadas, mas sim sugere possíveis itens que podem ser auditados, rastreados ou logados. Estes itens, então, devem ser avaliados pelos gestores do produto.

1. Exemplos de eventos que podem ser registrados

- Acessos a determinadas telas ou seções do sistema;
- Acesso a informações com alguma restrição (Ex: documentos sigilosos, dados pessoais...);
- Operações de inclusão, alteração ou exclusão de registros no banco de dados;
- Alteração de perfil de acesso (para sistemas que possuem acesso com diferentes perfis);

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 23 de 37	Revisão: 03	Publicação: 11/2021

- Execução de jobs e tarefas automatizadas.

2. Exemplos de informações que podem ser armazenadas, relativas a cada evento


- Data e hora;
- Usuário que efetuou a operação;
- Endereço IP;
- Identificador da sessão do usuário (quando aplicável Ex: cookie);
- Tela (página) do sistema de onde a operação foi realizada;
- Identificador da instância (para sistemas clusterizados);
- Para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;
- Parâmetros informados pelo usuário (Ex: parâmetros GET ou POST), tomando cuidado de não armazenar dados sensíveis, como senhas;
- Tempo de resposta do sistema;
- Para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada, etc.

12.6 – Prevenção, Reação e Mitigação de Falhas de Segurança

Esta seção apresenta diretrizes para a realização de procedimentos que garantam uma reação adequada à ocorrência de falhas de segurança. Detalha-se o emprego de backups, testes e tratamento de ocorrências.

1. Backups

- Deve-se definir um procedimento estruturado para a restauração de backups.
- Deve-se definir e capacitar responsáveis pela recuperação dos backups.
- Deve-se criar baselines das versões do sistema, facilitando a recuperação ágil para uma versão anterior.
- Deve-se realizar simulações de restauração de dados continuamente.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 24 de 37	Revisão: 03	Publicação: 11/2021

2. Testes


- Deve-se realizar testes manuais de segurança antes de cada versão do software que modifique sua estrutura (telas de login, serviços não autenticados, novos formulários com interação com o usuário, etc.).
- Deve-se garantir, através de testes automatizados, que os serviços e dados sigilosos estejam protegidos e disponíveis apenas para os usuários detentores das informações.
- Deve-se elaborar uma política de testes, automatizados ou não, visando a garantia de não vulnerabilidade aos principais ataques conhecidos em sistemas.
- Deve-se definir cenários de testes voltados à garantia dos requisitos não funcionais do software, preferencialmente realizado por uma equipe de testes diferente da equipe de desenvolvimento do software, com intuito de se evitar vícios.
- Deve-se definir cenários de testes, principalmente nos aspectos de segurança, para os casos de atualizações na arquitetura do sistema (servidores de aplicação, banco de dados, versões de browser, versões de sistema operacional, etc.).

3. Ocorrências

- Deve-se manter procedimento planejado para imediata indisponibilização do sistema e realização de manutenção corretiva.
- Deve-se definir uma política de acompanhamento pós-correção de ocorrências de falha de segurança.
- Deve-se utilizar lições aprendidas nas ocorrências passadas para revisar a política de testes e incrementar segurança dos sistemas.

4. Controles

- Deve haver controles que previnam erros de operação, perda, ou vazamento de informações. Todo sistema deve ser documentado, tornando sua implantação e operação independente de conhecimentos informais.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 25 de 37	Revisão: 03	Publicação: 11/2021

- Sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados sensíveis. Devem ser estabelecidos controles para monitorar e corrigir as vulnerabilidades e falhas desses.

12.7 – Ambiente de Desenvolvimento


Esta seção apresenta diretrizes para a instalação, configuração e gerenciamento de ambientes de desenvolvimento de sistemas.

1. Acesso ao Código-Fonte

- Diretivas para controle de acesso dos desenvolvedores ao código-fonte das aplicações. Quanto ao sigilo do código-fonte dos sistemas desenvolvidos, devem ser, por padrão, de livre acesso aos servidores da Vector. As demais situações deverão ser analisadas, projeto a projeto, pelos gestores.
- Deve-se utilizar um sistema de controle de versão com controle de acesso e recuperação em caso de falhas. (Ex.: Microsoft Team Foundation Server).

2. Separação de Ambientes

- Diretivas para a separação de ambientes de desenvolvimento/testes/homologação (DEV / TESTE / HOM) do ambiente de produção (PROD).
- As aplicações desenvolvidas devem considerar o uso de repositórios seguros de dados, especialmente na forma de banco de dados com acesso controlado ou arquivos criptografados, quando o uso de banco de dados não for possível/desejável. Parametrização para Proteção de Dados.
- Deve-se utilizar bancos de dados distintos para cada ambiente.
- Deve-se utilizar servidores de aplicação/web distintos para cada ambiente.
- Deve-se prover acesso ao ambiente de Desenvolvimento/Testes/Homologação apenas aos integrantes da equipe de desenvolvimento e aos interessados no projeto (stakeholders).
- Deve-se realizar testes periódicos para assegurar a segurança do ambiente de desenvolvimento/testes/homologação.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 26 de 37	Revisão: 03	Publicação: 11/2021


- Não se deve fornecer as senhas de acesso ao ambiente de produção aos desenvolvedores.

12.8 – Proteção de Dados

Esta seção apresenta diretrizes para a configuração de proteção a dados sensíveis. São detalhados parâmetros para criptografia, hash e gerenciamento de senhas.

1. Criptografia e Hash

- Devem ser estabelecidos controles criptográficos para proteger a confidencialidade, autenticidade ou integridade das informações. Faz-se necessária a documentação do uso de chaves, quando necessário.
- Diretrizes para a configuração e utilização de algoritmos de criptografia e hash visando prover confidencialidade a dados.
- Dados sigilosos e sensíveis devem ser criptografados sempre que possível. O método de criptografia empregado deve obedecer às particularidades dos dados e de sua utilização, seguindo os parâmetros aqui listados.
- Deve-se utilizar hashes criptográficos sempre que possível, sobretudo nos seguintes casos: verificação da integridade de dados; armazenamento e verificação de senhas; provimento de identificador “único” para objetos em um sistema e geração de números pseudo-aleatórios.
- Deve-se utilizar um método criptográfico que siga o princípio de Kerckhoffs. O método de encriptação e seus parâmetros devem ser públicos e estar documentados, somente a chave criptográfica deve ser mantida em sigilo.
- Não se deve utilizar um cifrador que admita um método conhecido para quebra da chave criptográfica (força bruta), baseada em tentativa e erro.
- Não se deve utilizar o modo de cifrador de bloco electronic codebook (ECB) ou modos menos seguros.
- Não se deve utilizar um tamanho da chave menor que 128 bits (cifrador simétrico) ou 1024 bits (cifrador assimétrico).
- Não se deve utilizar função de hash sem algum tipo de salt.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 27 de 37	Revisão: 03	Publicação: 11/2021

- Não se deve utilizar algoritmos considerados obsoletos para criptografia e hash criptográfico. Exemplos: MD5, SHA1, DES/3DES, RC2, RC4, MD4.
- Não se deve utilizar um tamanho da chave menor que 192 bits (cifrador simétrico) ou 2048 bits (cifrador assimétrico).
- Não se deve distribuir chaves criptográficas sem a utilização de uma infraestrutura de chave pública e, portanto, sem a utilização de um cifrador assimétrico.
- Não se deve utilizar um tamanho da chave menor que 256 bits (cifrador simétrico) ou 4096 bits (cifrador assimétrico).

2. Senhas


- Deve-se utilizar as normas de Senhas da Vector.

12.9 – Ciclo de Vida de Software

Esta seção apresenta diretrizes para reforço da segurança de software nas diferentes fases de seu ciclo de vida; projeto, codificação e manutenção. Traz ainda, diretrizes para a aplicação com as pessoas envolvidas nestas diferentes fases.

1. Projeto

- Deve-se empregar modelo de projeto de software que contemple:
- Etapa de modelagem de ameaças;
- Definição clara dos riscos de segurança;
- Nível de severidade que o comprometimento de dados sensíveis traria ao sistema e à instituição.
- Não se deve omitir, durante o projeto de desenvolvimento de sistema e sua execução, a definição de responsabilidades pela segurança de dados do sistema e como essa responsabilidade será verificada.
- Deve-se utilizar cronograma de projeto que contemple pontos de verificação de segurança do sistema desenvolvido ao longo de sua construção.

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 28 de 37	Revisão: 03	Publicação: 11/2021

2. Codificação

- Deve-se documentar, inclusive no código da aplicação, as medidas protetivas aplicadas no código-fonte, de modo a indicar precisamente o procedimento utilizado e suas peculiaridades.

3. Manutenção

- Não se deve habilitar as atualizações automáticas de software ou componentes utilizados na construção de um sistema, sob pena de introdução indevida de falhas de segurança.
- Não se deve modificar software de terceiros, salvo quando estritamente necessário. Controles de segurança internos podem ser invalidados. A mudança deve ser feita pelo desenvolvedor original do sistema sempre que possível.

4. Pessoal


- Deve-se proporcionar treinamento e capacitação de programadores para aquisição e revisão de princípios de segurança computacional e desenvolvimento de software seguro.

13 – GESTÃO DE INCIDENTES DE SEGURANÇA

O uso hoje de várias ferramentas tecnológicas potencializa os riscos cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das empresas.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores, etc.) como por exemplo:


- Ganhos financeiros através de roubo, manipulação ou adulteração de informações;
- Obter vantagens competitivas e informações confidenciais de clientes ou instituições concorrentes;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 29 de 37	Revisão: 03	Publicação: 11/2021

- Fraudar, sabotar ou expor a instituição invadida por motivos de vingança, idéias políticas ou sociais;
- Praticar o terror e disseminar pânico e caos;
- Enfrentar desafios e/ou ter adoração por hackers famosos.

Os invasores podem utilizar vários métodos para os ataques cibernéticos, destacam-se os mais comuns:

- Malware: softwares desenvolvidos para corromper computadores e redes;
- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações;
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido;
- Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;
- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;
- Ataques de DDOS (Distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 30 de 37	Revisão: 03	Publicação: 11/2021

utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços;

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada empresa. As consequências para as empresas podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais.


Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Empresas de qualquer tamanho podem ser impactadas, e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados sendo também essa necessidade um dos motivos da implementação desta Política na Vector.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;
- Conectividades como acesso a internet, Banco Central, Receita Federal, etc.;
- Informações sigilosas de clientes e da própria Vector;
- Componentes físicos, como servidores, estações de trabalho, notebooks, etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, a Vector tem voltado maior atenção para esse assunto com o objetivo de orientar seus colaboradores.


	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 31 de 37	Revisão: 03	Publicação: 11/2021

13.1 – Monitoramento e Gerenciamento de Incidentes

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Vector será monitorado, por meio de indicadores e geração de histórico, incluindo por exemplo e se aplicável de acordo com a solução adotada:

- Do uso da capacidade instalada da rede e dos equipamentos;
 - Tempo de resposta no acesso à Internet e aos sistemas críticos da Vector;
 - De períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Vector;
 - De incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
 - Das atividades de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).
- Nesse sentido, a Vector investirá continuamente em ferramentas robustas para monitoramento do ambiente, como também na manutenção de equipe especializada com expertise na área para garantir as regras mencionadas nesta Política, a Vector deverá:
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
 - Para os riscos associados a pharming, phishing, vishing e smishing, conduzir treinamentos e campanhas periódicas, bem como testes ao menos anualmente;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 32 de 37	Revisão: 03	Publicação: 11/2021

- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware se mantido servidor físico;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do Website da Vector, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Vector, ao menos semestralmente. Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Vector poderão ser acessados, caso o Comitê de Segurança Cibernética julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.


O processo de gerenciamento de incidente deve:

- Permitir a detecção, o mais cedo possível, e a capacidade de responder com a máxima eficácia para limitar os danos causados pelo incidente;
- Limitar as zonas de vulnerabilidade pela remediação de anomalias identificadas em algum ou todos os sistemas operacionais potencialmente afetados;
- Reter informações relevantes para posteriores investigações e coleta de provas;
- Compilar um registro de incidentes de segurança e estatísticas para uso na previsão de possíveis incidentes futuros;
- Identificar pontos de contato apropriados para o nível de severidade do ataque.

Uma vez que um incidente mal-intencionado for resolvido, uma análise deve ser feita para identificar a origem do ataque e iniciar procedimentos administrativos ou judiciais apropriados.

13.2 – Plano de Resposta a Incidentes e Informações Acerca da Segurança Cibernética


A Vector, deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios (“Plano”), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 33 de 37	Revisão: 03	Publicação: 11/2021

demais casos. Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte TI@vectorinf.com.br

Procedimento em caso de incidentes:

- Uma vez que o Responsável pela Segurança da Informação/Cibernética tenha sido acionado devido a um potencial incidente, este deverá convocar o Comitê de Segurança da Informação para que este delibere sobre a matéria.
- a) **Avaliação Inicial:** Nessa etapa inicial, aspectos e decisões fundamentais deverão analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.
 - b) **Incidente Caracterizado:** Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se:
 - será registrado um boletim de ocorrência ou queixa crime;
 - é necessário envolver consultor ou advogado externo;
 - haverá comunicação interna ou externa, em especial ao cliente que tenha sido afetado; e
 - houve prejuízo para a Vector;
 - além disso, o Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.
 - c) **Recuperação:** Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um call diário ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pelo Comitê, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.
 - d) **Retomada:** Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 34 de 37	Revisão: 03	Publicação: 11/2021

sistemas e eventuais mudanças e medidas de prevenção. A Diretoria deverá registrar o histórico em local adequado, como o sistema de gerenciamento.


14 – RESPONSÁVEIS A SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA

14.1 - Responsável pela Segurança da Informação / Cibernética

A Vector conta com um responsável para tratar e responder questões de segurança cibernética (“Responsável pela Segurança Cibernética”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Segue abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar ao Comitê de Segurança Cibernética os riscos residuais;
- Acordar com o Comitê de Segurança Cibernética o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 35 de 37	Revisão: 03	Publicação: 11/2021


- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Vector em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Vector, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Vector;
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Vector, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de Segurança Cibernética.

14.2 – Comitê de Segurança da Informação / Cibernética

O Comitê de Segurança da Informação / Cibernética será composto pelo:

- CEO
- Diretor Executivo
- Consultoria Segurança da Informação / Cibernética (Suporte ao Comitê)
- Gerente Cloud e Infraestrutura
- Responsável pela Segurança da Informação / Cibernética
- TI
- RH
- Acessória Jurídica

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 36 de 37	Revisão: 03	Publicação: 11/2021

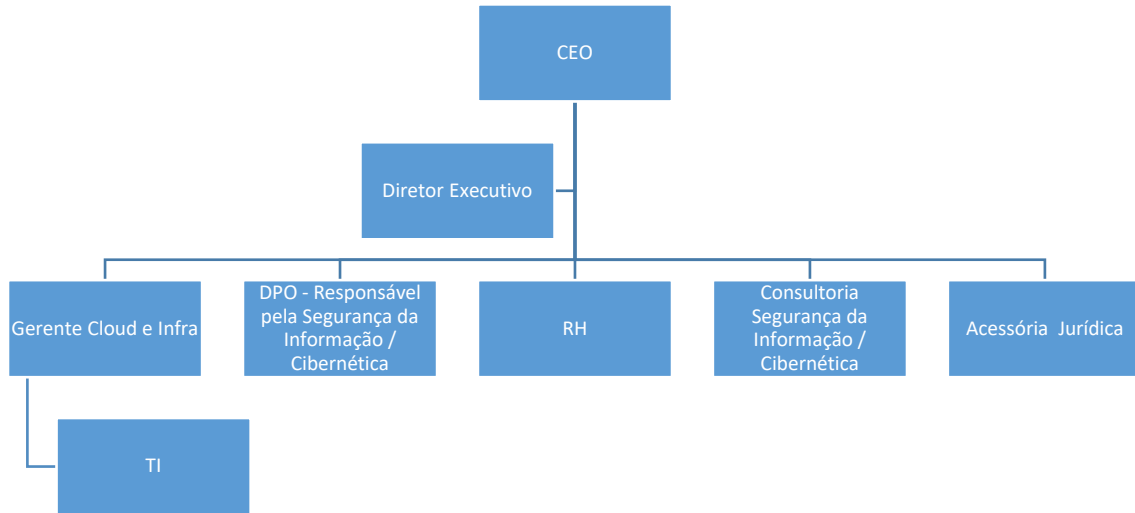



Figura 1 – Organograma do Comitê da Segurança da Informação / Cibernética

Esse Comitê tem como objetivo a supervisão e monitoramento das regras Segurança da Informação / Cibernética, conforme aqui previsto. E se reunirá no mínimo trimestralmente, ou sempre que necessário.

14.3 – Demais Atribuições – Todos Colaboradores

Demais Atribuições caberá a todos os Colaboradores conhecer e adotar as disposições das Políticas de Confidencialidade e Segurança da Informação e da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança da Informação / Cibernética, se for o caso.

Em caso de incidente que afete a segurança da informação / cibernética da Vector, o Colaborador deverá comunicar imediatamente ao Responsável pela Segurança da

	POLÍTICA COMPLEMENTAR DA SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA	Última Revisão – 04/2024		
		Página 37 de 37	Revisão: 03	Publicação: 11/2021

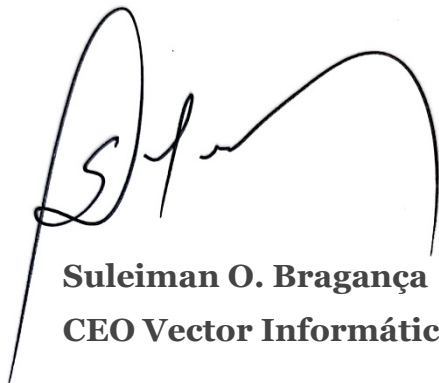
Informação / Cibernética, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

15 - CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política Complementar da Segurança da Informação - Cibernética deverão ser encaminhadas à Diretoria para avaliação e decisão.

Esta Política 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, novembro de 2021



Suleiman O. Bragança
CEO Vector Informática Ltda.