PSI

Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Barueri, fevereiro de 2015

1.0 - DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de Segurança da Informação – PSI da empresa Vector Informática Ltda, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. No entanto destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da empresa.

Esta versão pode ser alterada a qualquer momento, uma vez que os pontos apontados para mudanças sejam informados e discutidos com os demais colaboradores da Vector. Contudo a versão da PSI deve ser revisada a cada ano (no mínimo Anual), considerando a data de sua aprovação.

2.0 - CICLO DE APROVAÇÃO

Essa Política e todas os outros instrumentos normativos gerados a partir dessa Política, devem ser revisados sempre que se fizer necessário, no mínimo Anualmente.

Destacam-se as principais fases da Política de Segurança da Informação e no item 3.0 Versões sempre as atualizações necessárias que foram realizadas.

ELABORADOR	DATA
Rafael Nantes Flores	20/02/2015
REVISOR	
Marcelo Galdino Pereira	24/02/2015
APROVADOR FINAL	
Mandeleine Oliveira Bragança	26/02/2015

3.0 - VERSÕES

Versão	Data	Responsável	Controle das Modificações
1.0	02/2015	Mandeleine Bragança	Criação do Documento
1.1	02/2016	Mandeleine Bragança	Retirada do controle de acesso Físico ao Data Center
1.2	03/2017	Mandeleine Bragança	Revisão do Documento
1.3	02/2019	Marcelo Pereira	Revisão do Documento
1.4	09/2020	Rafael Flores	Revisão do Documento
2.01	06/2021	Emilson Moraes	Revisão do Documento
2.02	07/2021	Emilson Moraes	Revisão do Documento
2.03	08/2021	Rafael Flores	Revisão do Documento
2.04	04/2022	Lauma Costa	Revisão do Documento
2.05	04/2023	Lauma Costa	Revisão do Documento
2.06	04/2024	Lauma Costa	Revisão do Documento

Sumário

4.0 – SEGURANÇA DA INFORMAÇÃO COMO CULTURA ORGANIZACIONAL – DIVULGAÇÃO E CONSCIENTIZAÇÃO

Na Vector entendemos que segurança é parte principal da cultura e DNA da empresa. Toda a construção do negócio é feita em uma base sólida em segurança. Qualquer sistema, processo, procedimento e controle são concebidos em torno da segurança.

A cultura da segurança da informação deve ser adotada internamente por todos os colaboradores e parceiros. Para fornecedores, esta previsão deve estar explícita em cláusulas contratuais, assim como suas cadeias de relacionamento em primeiro nível.

O Treinamento aos colaboradores deve ser aplicados logo que inicia na empresa, e pelo menos 1 vez ao ano fazer uma reciclagem. Além disso, todos os colaboradores devem assinar o Termo de Compromisso em seguir todas essas normas descritas nessa Política.

Todos esses esforços convergem para a proteção dos ativos de Informação da “Vector”.

5.0 - GLOSSÁRIO

- Ativo: Algo que tenha valor para a organização;
- Evento: Acontecimento que acarreta na mudança do estado atual de um processo;
- Incidente: Evento que traz prejuízos à organização;
- Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos;

- Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização;

- Malwares: O nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador;

- SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para muitas pessoas;

- Phishing: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade;

- Mail bombing: Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível.

6.0 - DOCUMENTOS DE REFERÊNCIA

- Contrato de Trabalho Vector Informática;

- Código de Conduta Vector Informática;

- ABNT NBR ISSO/IEC 27002:2005;

- Lei Geral de Proteção de Dados (Lei nº 13.709).

7.0 - INTRODUÇÃO

A presente Política de Segurança da Informação – PSI está baseada nas recomendações da norma ABNT NBR ISSO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, e outras leis vigentes.

A informação é um ativo de grande valor para a empresa, por isso necessita ser adequadamente protegida.

"Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 17799:2005).

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

1. Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;

2. Integridade: Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;

3. Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

A Vector faz o acompanhamento do ciclo de atendimento dos clientes através do sistema de CRM, tornando essencial para o negócio que as informações sejam confiáveis e estejam devidamente protegidas.

Assim, é imprescindível a criação de uma política que normatize e direcione os procedimentos necessários para garantir a segurança das informações e a

consequente excelência no atendimento ao cliente, sendo este o caráter do documento ora apresentado.

8.0 - OBJETIVO DA PSI

"A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados" (ABNT NBR ISO/IEC 17799:2005).

A Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;
- O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores em todo o processo.

9.0 - POR QUE SE PREOCUPAR COM SEGURANÇA?

"Uma corrente é tão forte quanto seu elo mais fraco".

Não adianta a área da Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores, por exemplo, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

A área de Tecnologia da Informação é a responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver todos os colaboradores, independentemente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

10 - ALTA DIREÇÃO

A efetividade da Política de Segurança da Informação depende estritamente do comprometimento da alta direção.

É essencial que os responsáveis por liberar recursos, aplicar sanções, criar regras e portarias, apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados a cumpri-la.

A ordem expressa e o exemplo de cumprimento das cláusulas da PSI pela alta direção possibilita:

- A inexistência de exceções à regra;
- Que a PSI seja um ativo estratégico;
- Que a PSI componha a legislação interna da Vector;
- Que a PSI tenha ampla divulgação;

- Que a PSI seja incluída no processo de contratação de novos funcionários.

Caso está premissa não seja cumprida, a Política de Segurança da Informação se tornará apenas um documento obsoleto, existente na teoria e não adotado na prática.

11 - CLASSIFICAÇÃO

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

- Pública;
- Interna;
- Confidencial;
- Confidencial restrito.

1 – Pública: São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico. São exemplos de informação pública:

- Editais de licitação;
- Rotinas e agendas médicas;
- Campanhas de promoção à saúde.

2 – Interna: São informações disponíveis aos colaboradores da Vector para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo. São exemplos de informações internas:

- Memorandos, Portarias, Padrões, Políticas e Procedimentos internos;
- E-mails e lista telefônica internos;
- Avisos e campanhas internas.

3 – Confidencial: São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. São exemplos de informações confidenciais:

- Dados de clientes;
- Processos judiciais;
- Dados cadastrais de funcionários.

4 – Confidencial restrito: São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas ao CEO, gerentes e funcionários cujas funções requerem conhecê-las. São exemplos de informações confidenciais restritas:

- Atas de reunião da governança com a presidência da Vector;
- Indicadores e estatísticas dos processos de negócio da Vector;
- Resultado de auditorias internas.

12 - RESPONSABILIDADES

1 – Colaboradores: Será de inteira responsabilidade de funcionários, terceirizados e demais colaboradores da Vector:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Vector;
- Buscar o Setor de Gestão de Informação e Informática para esclarecimentos de dúvidas referentes à PSI;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela Vector;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Vector;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e procedimentos.

2 – Gestores de Pessoas e/ou Processos: Em relação à segurança da Informação, cabe aos gestores de pessoas e/ou processos:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da Vector;

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;

- Elaborar, com o apoio do Setor de Gestão de Processos e Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

- Tomar as decisões administrativas referentes aos descumprimentos da PSI da Vector.

3 – Subcomitê Gestor de Segurança da Informação: Cabe ao Subcomitê Gestor de Segurança da Informação:

- Propor melhorias, alterações e ajustes da PSI;

- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;

- Classificar e reclassificar o nível de acesso às informações sempre que necessário;

- Avaliar incidentes de segurança e propor ações corretivas.

O Subcomitê de Gestão de Segurança da Informação deverá ser composto por, no mínimo, um colaborador das seguintes áreas:

- Diretoria;
- Desenvolvimento;
- TI;
- RH; e
- Jurídico.

O CGSI reunir-se-á, ordinariamente, uma vez a cada seis meses e extraordinariamente sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a Vector.

4 - Setor de TI: Cabe ao Setor de TI:

- Definir as regras para instalação de software e hardware na Vector;
- Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede da Vector;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;

- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades, etc.;

- Promover, palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da Vector;

- Analisar criticamente incidentes de segurança em conjunto com o Subcomitê Gestor de Segurança da Informação;

- Manter comunicação efetiva com o Subcomitê Gestor de Segurança da Informação sobre possíveis ameaças e novas medidas de segurança;

- Buscar alinhamento com as diretrizes da organização.

5 – DPO – Encarregado de Proteção de Dados: Cabe ao DPO:

Dentre suas várias responsabilidades, todas previstas nos incisos do artigo 41, § 2º, da LGPD, as atividades do DPO consistem em:

I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. receber comunicações da autoridade nacional e adotar providências;

III. orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

13 - COMITÊ

O Comitê Gestor de Segurança da Informação é responsável pela elaboração e revisão periódica da Política de Segurança da Informação e normas relacionadas, tendo sua organização, composição, competências e funcionamento definidos nesta Política.

Atribuições do Comitê:

- Esclarecimento sobre questões não contempladas nessa Política e normas relacionadas;
- Monitorar a execução dessa Política, e do Plano de Continuidade de Negócios, sob a perspectiva da segurança da informação para sugerir e recomendar alterações que se façam necessárias;
- Dirimir dúvidas e deliberar sobre questões não contempladas pela política de segurança da informação ou pelas normas a ela relacionadas;
- Promover a cultura de segurança da informação, com a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação;
- Avaliar as informações recebidas do monitoramento e da análise crítica dos incidentes de segurança da informação, e recomendar ações apropriadas como resposta para os incidentes de segurança da informação;
- Emitir pareceres e manifestar-se sobre qualquer assunto relativo à política de segurança da informação e quando solicitado pela administração superior;
- Proposição da implantação de soluções para eliminação ou minimização de riscos;

- Elaboração de propostas de normas complementares e políticas de uso dos recursos de informação, em todo o seu ciclo de vida, tecnológicos ou não, tais como:

1. Acesso aos recursos de rede, inclusive internet;

2. Uso adequado de correio eletrônico (e-mail), estações de trabalho e dispositivos móveis fornecidos pela Vector;

3. Uso e instalação de softwares;

4. Monitoramento e auditoria dos recursos de tecnologia da informação;

5. Plano de continuidade do negócio; e

6. Tratamento e resposta a incidentes em redes computacionais.

Uma vez por ano, será feito uma eleição para a composição do Comitê de Segurança da Informação.

No anexo V – está a composição atual do Comitê de Segurança a Informação da Vector.

14 - UTILIZAÇÃO DA REDE

O ingresso à rede interna da Vector deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

Assim, é preciso que sejam instauradas algumas regras, listadas a seguir:

1. A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade da Vector, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores;

2. A Internet sem fio deverá ser segregada, garantindo o isolamento da rede interna, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; poderá ter outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam/podem ter acesso aos dados internos. A definição de qual rede o usuário deverá ingressar ficará a cargo do TI após análise dos requisitos de acesso;

3. A concessão de acesso à rede sem fio para acesso apenas à Internet se dará através de preenchimento de formulário disponível na página http://vectorinf.com.br, aba “Suporte Técnico”, opção “Solicitação de Acesso WiFi. O usuário deverá preencher o formulário e encaminhá-lo impresso ao TI, devidamente assinado pelo chefe do setor. Ficam estabelecidos os seguintes períodos de acesso:
    - 1 ano para colaboradores,
    - 6 meses para estagiários; e
    - 1 semana para visitantes.

4. O RH ficará responsável por notificar formalmente TI sobre desligamentos de colaboradores, para que os acessos dos mesmos sejam revogados;

5. A Vector reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

6. Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da Vector, que pode analisar e, se necessário, bloquear

qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação;

7. A Internet disponibilizada pela Vector aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada pelo chefe e não prejudique o andamento dos trabalhos nos setores;

8. Apenas colaboradores devidamente autorizados a falar em nome da Vector para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica, etc.;

9. É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;

10. Os colaboradores com acesso à Internet só poderão fazer o download programas necessários às suas atividades na Vector e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pelo TI;

11. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pela TI;

12. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Vector para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

13. Como regra geral, materiais de cunho sexual não poderão ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

14. Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

15. Os colaboradores não poderão usar os recursos da Vector para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;

16. Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µtorrent e afins);

17. Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc;

18. Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;

19. Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando a TI deverá estar devidamente ciente e concedido autorização para tal;

20. Os arquivos inerentes a Vector, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;

21. Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

22. Haverá geração de relatórios de sites e downloads acessados por usuário.

15 - POLÍTICA DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1. A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;

2. A senha inicial só será fornecida ao próprio colaborador, pessoalmente, sendo exigida a troca ao primeiro uso. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;

3. É proibido o compartilhamento de login para funções de administração de sistemas;

4. As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

5. As senhas deverão seguir os seguintes pré-requisitos: - Tamanho mínimo de oito (8) caracteres; - Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais; - Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc).

6. O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;
- Mudança de função do colaborador;
- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

7. Para os cancelamentos acima mencionados, o RH ficará responsável por informar prontamente o TI acerca dos desligamentos e mudança de função dos colaboradores.

15.1 – AUTENTICAÇÃO

A autenticação é o processo pelo qual um sistema ou serviço confirma que uma pessoa ou dispositivo realmente é quem afirma ser e por meio do qual o acesso ao recurso solicitado é autorizado. É necessário a autenticação antes do uso de qualquer conta.

A Autenticação Multifatorial, permite melhorar a segurança da Vector, este método requer que todos os membros com contas da Vector se autentiquem por meio do aplicativo interno Jumpcloud – domínio em nuvem (Cloud Domain). Que é o único meio de IDM (gestão de usuários e senhas).

E a ferramenta que controla o SSO (Single Sing-On), e também o MFA (Multi Fator de Autenticação), sendo todos os sistemas autenticados pelo Jumpcloud, inclusive a VPN da Vector.

16 - GESTÃO DE CONTAS ADMINISTRATIVAS

Entende-se por contas administrativas, contas padrões de acesso administrativo, root ou de serviço com privilégios que possam obter, modificar, comprometer ou danificar dados corporativos ou serem usados para obter acessos não autorizados.

Exemplo: Administrador, root, sysadmin, local admin, SA, etc.

Senhas que se enquadram neste perfil devem seguir as seguintes normas e práticas:

1. Serem renomeadas para um nome não trivial;
2. Serem compostas de um mínimo de 16 caracteres contendo letras maiúsculas, letras minúsculas, números e símbolos;
3. Serem geradas randomicamente através de gerador de senhas;
4. Serem trocadas a cada 12 meses;
5. Não podem ser reutilizadas;
6. Salvas em local seguro, físico ou digital, livre de incêndios ou acidentes naturais com acesso apenas para administradores qualificados, diretoria e presidência;
7. Contas "guest" devem ser desativadas.

17 - DO USO DOS ATIVOS DE TI (FERRAMENTAS CORPORATIVAS)

A Vector poderá fornecer ao colaborador conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha celular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho. O uso destas ferramentas estará sujeito a esta Política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Comitê de Segurança da Informação.

Como política de nível de acesso à Informação, utilizamos a premissa de *"menor privilégio possível"*. O colaborador somente terá acesso aos aplicativos e Informações que forem estritamente necessários para a realização do seu trabalho. É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.

O colaborador é responsável pelos ativos de TI da Vector, bem como pelas Informações que inserir em tais ativos.

18 - ACESSO E USO DA INTERNET

A Vector poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis. É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área de Segurança da Informação da Vector.

Essa aprovação é uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantirmos que somente ferramentas e fabricantes que possuam

alta maturidade em Segurança da Informação, proteção de dados e políticas claras de privacidade, sejam incorporados à lista de ferramentas e fornecedores aprovados. Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de Segurança da Informação. Da mesma forma, não será permitido o download de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação. O colaborador deve consultar o departamento de TI antes de fazer o download de qualquer software de terceiros.

19 - CORREIO ELETRÔNICO (E-MAIL)

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso:

1. O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;

2. Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

3. É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;

4. É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

5. É proibido enviar qualquer mensagem por meios eletrônicos que torne a Vector vulnerável a ações civis ou criminais;

6. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

7. Produzir, transmitir ou divulgar mensagem que:

- Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
- Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

8. O uso de e-mails pessoais não é aceitável na máquina local.

9. O uso de e-mails pessoais no ambiente de data center não é permitido;

10. O uso de e-mail corporativo ou qualquer outra forma de acesso corporativo em equipamento pessoal, não é permitido em qualquer hipótese.

20 - USO DE ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

1. É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;

2. Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

3. É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe do TI;

4. As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas;

5. É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do TI;

6. É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do TI;

7. As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;

8. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão sempre serem armazenados em local próprio no servidor da rede em data center, o qual possui rotinas de backup e controle de acesso

adequado. Não é permitido armazenamento de documentos corporativos localmente;

9. Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;

10. É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

11. O TI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da empresa;

12. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

21 - USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo da Vector é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da empresa ou particular com prévia aprovação e permissão pelo TI, como: notebooks, tablets, smartphones e dispositivos de armazenamento.

Todas as regras do tópico “Estações de Trabalho” se enquadram nesta seção, adicionalmente a:

1. Fica autorizado o uso de dispositivos móveis para acesso à rede Guest de Internet da empresa mediante autorização do chefe imediato via memorando e prévio cadastro e liberação do TI;

2. O uso de dispositivos móveis para fins de acesso à rede de Guest de Internet da empresa será realizado mediante cadastro de usuário através do endereço htpp://vectorinf.com.br e autorização do chefe imediato (Ver item 13 – Utilização da Rede);

3. O departamento de TI deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que não estejam de acordo com a

legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem da empresa, não serão permitidos;

4. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;

5. O departamento de TI tem o direito de, periodicamente, auditar os equipamentos utilizados na empresa, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados na empresa;

6. É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no equipamento, salvo exceções de aplicativos específicos autorizados pelo TI;

7. É de responsabilidade do proprietário usar somente aplicativos legalizados em seus equipamentos;

8. Não podem ser executados nos dispositivos aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;

9. É proibido transitar ou manter arquivos corporativos nos dispositivos pessoais;

10. É proibido transitar ou manter arquivos corporativos nos dispositivos da empresa;

11. É proibido o uso de dispositivos pessoais para acesso à rede corporativa local;

12. É proibido o uso de dispositivos pessoais para acesso à rede corporativa em nuvem;

13. É proibido o uso de dispositivos pessoais para finalidade de trabalho;

22 - USO DE IMPRESSORAS

O uso de impressoras na Vector deve seguir algumas regras:

1. É proibida a impressão e cópia de documentos de cunho pessoal e/ou ilegal;

2. A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica do TI;

3. O chefe de cada setor / unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões/cópias excessivas;

4. As impressoras devem estar ligadas na energia através dos seus transformadores e serão proibidas intervenções desta natureza por parte de qualquer colaborador que não seja do TI.

23 - POSTURA GERAL DE PRIVACIDADE

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio. É expressamente proibido o acesso a quaisquer Informações de clientes, colaboradores ou qualquer registro nos sistemas de Informação da Vector sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

24 - MONITORAÇÃO

A Vector se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de Informação para garantir o cumprimento desta e outras políticas da empresa. Os ambientes internos da Vector também podem sofrer

gravação audiovisual com o propósito principal de gerenciar a segurança do perímetro interno da empresa contra incidentes de segurança de qualquer natureza.

25 - ACESSO AO ESCRITÓRIO E ESCOLTA DE VISITANTES

O acesso aos nossos escritórios NÃO pode ser feito por pessoas DESACOMPANHADAS. O anfitrião do visitante deverá acompanhá-lo, DESDE a chegada na recepção da Vector, até a entrada no escritório. Quem não possui biometria cadastrada ou crachá de acesso, sempre terá que ser acompanhado pelo seu anfitrião ou por um colaborador da Vector. Para colaboradores ou consultores externos que trabalhem mais de dois dias por semana no escritório, iremos cadastrar sua biometria ou crachá e liberar o acesso sem escolta.

26 - BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer. Assim, estabelecem-se as regras:

1. Todo sistema ou informação relevante para a operação dos negócios da Vector deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da empresa;

2. As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e informar a TI sobre a necessidade de backup dos mesmos, sugerindo o tempo de retenção destas cópias;

3. Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial,

períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

4. As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;

5. Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

6. A TI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;

7. Na situação de erro de backup e/ou restauração é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

27 - SEGURANÇA DO AMBIENTE DE TI

Estrutura Física do Data Center As máquinas (servidores) que armazenam sistemas da Vector estão em área protegida.

1. **Data Centers in loco:**

- Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do Data Center;

- A entrada aos Data Centers tem acesso devidamente controlado e monitorado;

- As permissões de acesso físico às áreas restritas do Data Center devem ser mensalmente revisadas;

- As áreas do Data Center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;

- A porta do Data Center deve permanecer fechada, com mecanismo de autenticação individual quando possível;

- O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Segurança e mediante supervisão;

- O acesso ao Datacenter sem as devidas identificações só poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando;

- Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável

pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter;

- O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais;

- Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;

- A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a mesma deve ser autorizada pelo Subcomitê Gestor de Segurança da Informação.

2. Estrutura Lógica do Data Center:

- Na política de segurança da Informação estabelecida pela Vector, define-se que os analistas de TI, mediante ciência do Subcomitê Gestor de Segurança da Informação, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo às atribuições de sua área de atuação;

- O objetivo da segurança lógica no Data Center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados;

- Somente os colaboradores credenciados e autorizados pelo Subcomitê Gestor de Segurança da Informação podem ter acesso aos dados armazenados;

- Os logs dos ativos de rede devem ser monitorados constantemente a fim de evitar acessos indevidos.

28 – GESTÃO E DESCARTE DE MÍDIAS DE ARMAZENAMENTO DE DADOS

Entende-se por mídias de armazenamento de dados, qualquer dispositivo não volátil que possa ser usado para cópia, armazenamento ou transferência de dados da empresa, como disco rígido, pendrive, flashdrive, microsd, cd, dvd, ou qualquer outro meio não citado, futuro ou histórico que sirva para essa finalidade.

1. Por opção e política desta empresa, todos os dados corporativos são armazenados apenas em ambiente hermético de rede privada em nuvem e disponibilizado acesso externo por canal seguro via "Área de Terminal Remota" com VPN, não sendo tecnicamente disponibilizado nem politicamente permitido a cópia, armazenamento ou transferência permanente ou transitória dos mesmos em qualquer meio externo à nossa nuvem privada, sendo externos via Internet ou localmente em dispositivos locais.

2. Não é disponibilizada nem permitida a utilização de mídias externas para armazenamento de dados corporativos.

3. Não é permitido o armazenamento de dados corporativos em mídias internas, pessoais ou corporativas.

4. Todas as mídias instaladas fisicamente nos desktops e notebooks da empresa devem ser disponibilizados de forma criptografada.

5. Para descarte ou repasse de mídias de armazenamento deve-se operacionalizar a formatação física dos mesmos, setor por setor, ou em caso de defeito, desmontados e danificados via material perfurando, uso de micro-ondas ou substância corrosiva.

29 - VIOLAÇÃO DAS POLÍTICAS E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

1. Advertência verbal:

- O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da Vector e será recomendado à leitura desta Norma.

2. Advertência formal:

- A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida;
- A segunda notificação será encaminhada para a chefia imediata do infrator.

3. Demissão:

- Uma vez verificada a não observância da política de segurança da empresa pelo colaborador, o mesmo será desligado da empresa sendo validado ou não a necessidade e possibilidade de Justa Causa, inclusive podendo o mesmo ser Processado em análise de uma causa grave.

Observação: A qualquer momento que for verificado uma causa grave cometida ou verificado uma inviabilidade do colaborador permanecer na empresa, o mesmo será desligado podendo o mesmo ser processado.

30 - EXTRAVIO DE INFORMAÇÃO

Qualquer evento de perda, extravio ou roubo de Informações, devem ser reportados IMEDIATAMENTE ao Comitê de Segurança da Informação, por meio do http://vectorinf.com.br, aba “Suporte Técnico”, ou através do canal aberto.

31 - CANAL ABERTO

A Vector Informática deixa um canal aberto, para que todos possam contribuir com sugestões e também caso precise denunciar algo irregular que fere a nossa política de Segurança da Informação e Proteção de Dados. Canal de comunicação: faleconsoco@vectorinf.com.br

32 - CONSIDERAÇÕES FINAIS

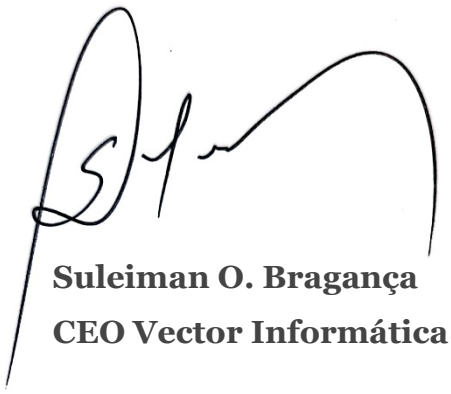
As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à Diretoria para avaliação e decisão.

Esta PSI 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.

33 - APROVAÇÃO

Esta Política de Segurança da Informação foi elaborada pelo Diretor Executivo Rafael Flores e pelo Gestor da área de Tecnologia da Informação da Vector Informática sr Emilson Queiroz e teve a participação do Comitê da Segurança da Informação da Vector. Essa Política foi aprovada na reunião realizada em 26/02/2015, com a participação do CEO sr Suleiman Bragança, e todo o Comitê da Segurança da Informação.
A Política de Segurança da Informação da Vector Informática entra em vigor a partir da data de sua publicação, e terá que ser revista e melhorada anualmente.

Barueri, 26 de fevereiro de 2015



Suleiman O. Bragança
CEO Vector Informática Ltda.

ANEXO I – TERMO DE COMPROMISSO

Nome:	
CPF:	RG:
e-mail:	Fone:

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes;
2. Utilizar adequadamente os equipamentos da Empresa, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações;
3. Não revelar, fora do âmbito profissional, fatos ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico;
4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico;
5. Manter cautela quanto à exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos;
6. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de sanções disciplinares cabíveis.

Barueri, _____ de _____ de _____.

_____

Assinatura do Colaborador

ANEXO II – TERMO DE RESPONSABILIDADE DE USO DE NOTEBOOK PARTICULAR NA REDE CORPORATIVA

Nome:	
CPF:	RG:
e-mail:	Fone:

1. O presente termo objetiva a cessão de acesso à rede corporativa da Vector ao colaborador acima identificado;
2. O presente instrumento vigorará imediatamente a partir da assinatura deste;
3. O colaborador ficará responsável por: - Obedecer às normas vigentes da Política de Segurança da Informação;

- Toda e qualquer manutenção/despesa que for necessária para o pleno funcionamento do equipamento;
- Possuir um aplicativo Antivírus devidamente atualizado;
- Instalar apenas aplicativos com licença de livre distribuição, ou que o mesmo tenha adquirido a sua licença;
- Não copiar, reproduzir ou distribuir documentos, arquivos, programas ou qualquer informação que forem de direito da Vector;
- Todo e qualquer prejuízo que, por sua culpa, na utilização do equipamento, vier causar a terceiros, durante o tempo de vigência deste Termo.

Barueri, _____ de _____ de _____.

_____

Assinatura do Colaborador

ANEXO III – TERMO DE RESPONSABILIDADE DE ADMINISTRADOR DE PERMISSÕES DE ACESSOS, AUTORIZAÇÕES, DIREITOS E PRIVILÉGIOS

Nome:	
CPF:	RG:
e-mail:	Fone:

1. O presente termo objetiva as responsabilidades de Administradores de Direitos e Privilégios à rede corporativa da Vector ao colaborador acima identificado;
2. O presente instrumento vigorará imediatamente a partir da assinatura deste;
3. O colaborador ficará responsável por:

- Obedecer às normas vigentes da Política de Segurança da Informação;
- Atribuir acessos e autorizações seguindo o "Princípio de Menor Privilégio" (POLP) e "Segregação de Função";
- Separar contas de administradores das contas de usuários convencionais;
- Criar grupos de usuários/permissões, vincular permissões aos grupos e incluir o usuário ao grupo;
- Criar contas de acesso com o menor privilégio possível;
- Toda permissão de acesso deve ser autorizado por um superior do usuário requerente e concedido até o limite do privilégio do autorizador;
- Liberar apenas os acessos necessários para que as tarefas possam ser cumpridas;
- A autorização deve ser concedida ao usuário apenas pelo tempo necessário para o desenvolvimento da função e removida quando não mais necessária;
- Toda conta de acesso deve ser criada individualizada, e não agrupada, a fim de manter a rastreabilidade;

- Executar auditorias periódicas a fim de validar o seguimento das normas acima evidenciadas.

Barueri, _____ de _____ de _____.

_____

Assinatura do Colaborador

ANEXO IV – TERMO DE RESPONSABILIDADE PARA EMPRESAS

As empresas prestadoras de serviço devem ser orientadas para que mantenham documento similar em seus arquivos, assinado pelos colaboradores por ela contratados para prestar serviços na Vector, devendo o texto abaixo ser incluído nos contratos de prestação de serviço:

1. "Fica a Contratada, responsável pela orientação dos colaboradores por ela indicados para trabalharem junto à contratante, no que diz respeito ao cumprimento das Políticas de Segurança da Informação e Cibernética da Contratante e no cumprimento das legislações e regulações aplicáveis.

2. Fica também a Contratada corresponsável pela utilização das senhas e uso das informações por parte dos colaboradores por ela contratados e disponibilizados para atuação junto à Contratante, de acordo com o termo de responsabilidade assinado pelo colaborador da Contratada. Esta corresponsabilidade estende-se inclusive aos foros judiciais, sob todos os aspectos, inclusive o do direito das obrigações.

Barueri, _____ de _____ de _____.

_____

Assinatura do Colaborador

ANEXO V – COMITÊ DA SEGURANÇA DA INFORMAÇÃO

Segue a composição do Comitê da Segurança da Informação, especificando a função de cada participante e as principais atribuições.

Nome	Cargo	Função	Atribuições
Suleiman Bragança	CEO	Apoio a toda a estrutura da empresa	*Aprovar a Política de Segurança da Informação e suas atualizações.
Rafael Flores	Diretor Executivo	Apoio Desenvolvimento de Sistema	*Cria regras e portarias e aplica as sanções para garantir a Segurança da Informação. *Responsável por liberar recursos, fazer os planejamentos e dar a continuidade do negócio. *Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos. *Monitorar a execução dessa Política, e do Plano de Continuidade de Negócios, sob a perspectiva da segurança da informação para sugerir e recomendar alterações que se façam necessárias.

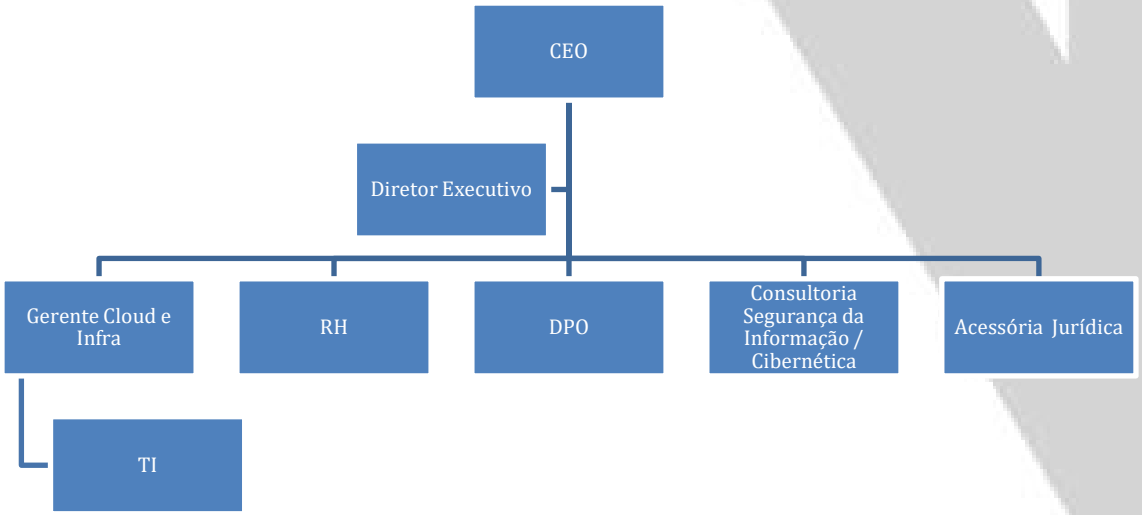
			*Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação.
Lauma Costa	DPO - Responsável pela Segurança da Informação / Cibernética	Segurança da informação / cibernética	*Providenciar e organizar todos os procedimentos para manter a segurança da informação – cibernética.
Emilson Queiroz	Gerente Cloud e TI	Apoio a Governança de TI	*Fazer a gestão da segurança das informações na Cloud e toda a estrutura da rede da empresa. *Classificar e reclassificar o nível de acesso às informações sempre que necessário. *Proposição da implantação de soluções para eliminação ou minimização de riscos.
Andre Morais	TI Infra	Apoio de Infraestrutura da TI	*Elaborar junto com o Gerente Cloud / TI e todo o comitê, os procedimentos de segurança da informação, fornecendo as informações necessárias e mantendo-os atualizados.

			*Fazer a gestão dos acessos e responsável para que as informações estejam sempre acessíveis para o uso legítimo de pessoas autorizadas. *Avaliar incidentes de segurança e propor ações corretivas. *Elaboração de propostas de normas complementares e políticas de uso dos recursos de informação, em todo o seu ciclo de vida, tecnológicos ou não, tais como: - Acesso aos recursos de rede, inclusive internet; - Uso adequado de correio eletrônico (e-mail), estações de trabalho e dispositivos móveis fornecidos pela Vector; - Uso e instalação de softwares; - Monitoramento e auditoria dos recursos de tecnologia da informação; - Plano de continuidade do negócio; e -Tratamento e resposta a incidentes em redes computacionais.

Malila Oliveira	RH	Apoio aos colaboradores	*Divulgar e disponibilizar a todos os colaboradores material que divulga as regras da Segurança da Informação da Vector. Promover a cultura de segurança da informação, com a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação. *Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da Vector. *Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade. *Tomar as decisões administrativas referentes aos descumprimentos da PSI da Vector.

Escritório Jurídico	Assessores Jurídicos	Apoio Jurídico	Atualizar sobre as leis da Segurança da Informação.
Consultoria Segurança da Informação / Cibernética	Consultores SI	Apoio Segurança da Informação	Orientar e atualizar todos os processos para a Segurança da Informação.

ORGANOGRAMA DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO



Barueri, abril de 2024