‘	Elaborado	Verificado	Aprovado	HISTÓRICO DE REVISÔES	
Valido	NELSON NASCIMENTO	JULIANA LOBATO	KLEBER CARAMASCHI	REV.04 20/05/2021	Revisão Geral - Melhoria
20/05/2021	CONSULTOR	GERENTE GERAL	DIR. EXECUTIVA		
	20/05/2021	20/05/2021	20/05/2021		

Sumário

1. OBJETIVO

A Política de Segurança da Informação é a declaração formal do VALIDE SOLUÇÕES sobre o compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos seus funcionários, stakeholders, parceiros e/ou fornecedores.

2. ABRANGÊNCIA

Aplica-se a todas as unidades e setores do VALIDE SOLUÇÕES .

3. DEFINIÇÕES E LEGISLAÇÃO

1.1 Legislação e Normas

ISO 27000:2014 – Sistema de Gestão de Segurança da Informação: Visão geral e vocabulário;

ISO 27001:2013 – Sistema de Gestão de Segurança da Informação: Requisitos da norma;

ISO 27002:2013 – Tecnologia da Informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

Lei n° 9.609/98 – Lei do Software;

Lei n° 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD)

1.2 Definições

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Agentes de tratamento: o controlador e o operador;

Tratamento: toda operação realizada com dados pessoais e/ou sensíveis;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

1.3 Classificação da informação

A informação classifica-se em:

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Anonimização: utilização de meios técnicos ou tecnologia razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Pseudoanonimização: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

Dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Informação pública: quando possui caráter informativo, comercial ou promocional. É destinada ao público externo e/ou ocorre devido ao cumprimento de legislação vigente que exija sua publicidade;

Confidencial: trata-se de dado crítico para os negócios ou clientes. A divulgação não autorizada ou vazamento pode causar impactos de ordem financeira, imagem, operacional, sanções administrativas, civis e/ou criminais;

As informações confidenciais devem ser sempre restritas a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores;

Interna: é aquela que não se tem interesse em divulgar e o acesso por parte de indivíduos externos a empresa deve ser evitado.

Caso essa informação seja acessada indevidamente, poderá causar danos a estratégia, posicionamento ou imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços.

Restrita: é a informação que deve ser acessada e/ou disponibilizada somente para usuários autorizados e envolvidos com o assunto;

A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização;

Cópia controlada: trata-se da revisão/ versão mais atualizada de um determinado documento;

Cópia não controlada: cópia com revisão mais atualizada no momento de sua emissão, mas que não se pode responder por seu controle posterior a emissão, ex.: POPs protocolados em departamentos de Vigilância Sanitária ou outros órgãos públicos;

Cópia obsoleta: cópia com revisão desatualizada que deve ser recolhida ao arquivo sob qualquer fim.

1.4 **Cibersegurança e ataques a informação**

- Cibersegurança é a prática de proteger ativos de informação, tais como: sistemas, computadores, servidores, entre outros, contra ameaças cibernéticas ou ataques maliciosos.

- Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Os hackers exploraram a falta de conhecimento do usuário.

A Engenharia Social manifesta-se de diversas formas, e podemos dividi-la em dois grupos, sendo:

Direta*:* caracterizada pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente. Nem sempre o engenheiro social é alguém desconhecido;

Indireta*:* caracterizada pela utilização de softwares, malwares ou ferramentas que visam a invasão de sistemas, como por exemplo, vírus, cavalos de Tróia (Trojan) ou através de sites e/ou e-mails falsos.

- Phishing: é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

4. RESPONSABILIDADES

2.1 **Todos os colaboradores, aprendiz legal, estagiários, fornecedores e prestadores de serviços**

- Cumprir fielmente a Política de Segurança da Informação;
- Em caso de dúvidas, buscar orientação com superiores diretos e/ou comitê interno de segurança da informação;
- 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 aprovadas pela empresa;
- Cumprir a lei e as normas relativas à proteção de Dados Pessoais da empresa;
- Comunicar imediatamente a empresa quando tiver conhecimento de vazamento de informações, por quaisquer que sejam os motivos, descumprimento ou violação de dados da empresa e/ou pessoais dos clientes internos e/ou externos ou da política de segurança da informação da empresa através do canal **dpo@validesoluções.com.br** e/ou informando sua chefia direta e/ou procurando quaisquer dos membros do Comitê de Segurança da Informação.

2.2 Gerências e coordenações

Cabe às Gerências e Coordenações cumprir e fazer cumprir esta política, além de assegurar que suas equipes possuam acesso e conhecimento a esta Política de Segurança da Informação.

Comunicar imediatamente a empresa quando tiver conhecimento de vazamento de informações, por quaisquer que sejam os motivos, descumprimento ou violação de dados da empresa e/ou pessoais dos clientes internos e/ou externos ou da política de segurança da informação da empresa através do canal **dpo@validesoluções.com.br** e/ou informando sua chefia direta e/ou procurando quaisquer dos membros do Comitê de Segurança da Informação;

2.3 Tecnologia da informação, comitê de segurança da informação e governança corporativa

Compete as áreas a propositura de ajustes, melhorias, aprimoramentos e modificações desta política da informação, devendo para tanto:

- **Convocar**, **coordenar, lavrar** atas, abrir não conformidades e tratá-las, **prover** apoio às reuniões que discutam a respeito desta Política de Informação;
- **Munir** a alta Diretoria de todas as informações relativas à segurança da informação;
- **Manter e conscientizar** sobre as políticas corporativas de segurança da informação, seus procedimentos e padrões;
- **Realizar** o planejamento e condução de capacitações periódicas com o objetivo de disseminar a cultura de segurança dentro da empresa, bem como de comunicar as atualizações eventualmente efetuadas nas políticas corporativas de segurança da informação, seus procedimentos e padrões;
- **Garantir** a concessão de acesso, término ou mudança de direitos de acesso à rede e aplicações críticas de acordo com o perfil de cada usuário;
- **Garantir** a melhoria de segurança da informação e segurança cibernética da organização através de projetos e iniciativas;
- **Conduzir** a gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinar as causas e os responsáveis, e realizar a comunicação interna e/ou externa dos fatos ocorridos.

2.4 Alta direção

A alta direção é responsável por supervisionar o desenvolvimento e implementação das políticas, procedimentos, controles de segurança da informação e segurança cibernética e são responsáveis por:

- **Aprovar** as políticas e procedimentos de segurança da informação, suas mudanças e/ou

atualizações;

- **Apoiar** para as iniciativas que vislubrem a segurança dainformação;
  - **Promover** a cultura em segurança da informação e cibernética na organização;
  - **Fornecer** os recursos necessários para o sistema de gestão de segurança da informação destinando rubrica própria.

2.5 Encarregado de Dados - DPO

O DPO é responsável por:

- **Servir** como ponto de contato entre a empresa, as autoridades competentes e grupos de interesses especiais, quais sejam conselhos de classe, sindicatos, sociedades e/ou associações cientificas e outros;
- **Receber** comunicações da autoridade nacional e adotar providências;
- **Treinar e orientar** os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- **Realizar** avaliações e auditorias regulares para garantir a conformidade com a LGPD;
- **Manter** registros das atividades de processamento de dados realizadas pela organização, especialmente sobre as não conformidades e exclusão de dados quando solicitados por seus titulares;
- **Aceitar** reclamações e comunicações dos titulares, prestar esclarecimentos e adotar as providências cabiveis;
- **Responder e informar** os titulares de dados pessoais sobre como seus dados estão sendo usados e quais medidas de proteção implementadas pela organização;
- **Assegurar** que os pedidos de acesso ou apagamento de dados feitos por titulares de dados pessoais, sejam atendidos ou respondidos, conforme necessário;
- **Executar** as demais atribuições determinadas pelo controlador ou estabelecidas em normas e Leis relacionadas.

2.6 Data Protection Expert (DPE)

- **Participar e orientar** sob a ótica de privacidade o Tratamento de Dados Pessoais a fim de validar a aderência aos requisitos da legislação e da regulamentação aplicáveis, além de garantir privacidade como um padrão;
- **Auxiliar** operacionalmente o monitoramento do cumprimento das regras internas e manutenção de KPIs (Key Performance Indicator) relacionados à proteção de dados e privacidade;

- **Auxiliar** na condução periódica de avaliações / auditorias de maturidade sobre as iniciativas de privacidade, identificando a evolução do programa e os gaps remanescentes e/ou novos;
- **Apoiar** a implementação dos planos de ação para correção de gaps das iniciativas de privacidade;
- **Apoiar** o preparo dos relatórios de impacto à proteção de Dados Pessoais (DPIA – Data Protection Impact Analysis) e a tomada de decisão alinhada aos requisitos desta Política;
- **Monitorar** as requisições dos Titulares de Dados Pessoais, a fim de garantir que sejam respondidas dentro do prazo;
- **Garantir** a manutenção das evidências de execução e implementação das iniciativas de privacidade, (princípio da responsabilização);
- **Auxiliar** as atividades e consultas ao DPO.

3 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A informação é um ativo importante para os negócios, possui valor para a organização e, consequentemente, necessita ser adequadamente gerenciada, tratada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

É fundamental para a segurança, proteção e salvaguarda das informações que os usuários mantenham comportamento seguro e consistente, alinhados com os valores da empresa, devendo assumir postura proativa e engajada no que diz respeito à proteção das informações.

A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é caracterizada por:

a) **Autenticidade:** garantia da identidade de quem está enviando a informação, ou seja, propriedade intelectual da informação. A fonte não foi alvo de mudanças ao longo do processo;

b) **Confidencialidade**: garantia de que a informação é acessível somente a pessoas interessadas/ parte do processo com acesso autorizado;

c) **Integridade:** salvaguarda a exatidão da informação e dos métodos de processamento;

d) **Disponibilidade:** garante que a informação esteja disponível para o uso legal e legítimo da informação.

A Política de Segurança da Informação da empresa VALIDE SOLUÇÕES é aprovada e revisada anualmente pela Alta Diretoria da empresa, com o intuito de sempre manter-se dentro da legislação vigente e alinhados as novas tendências tecnológicas de segurança.

4 SEGURANÇA DA INFORMAÇÃO NO NEGÓCIO

4.1 Acesso físico às salas restritas

Determina o perímetro e controle de acesso físico necessário para os ambientes que contenham dispositivos críticos, amostras biológicas, documentos sigilosos e dados pessoais ou sensíveis da empresa ou clientes.

A entrada em salas que comportem informações pessoais, sensíveis ou da empresa, são restritas e em caso de necessidade de entrada de terceiros, deverão estar acompanhados de pessoas autorizadas. Mesmo para funcionários, os acessos as salas restritas só serão permitidas aqueles com responsabilidade de executar tarefas relativas ao departamento;

É proibido o uso, nas dependências da empresa, de quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, sendo exceção quando partir de demanda da própria instituição e/ou feito a partir de autorização prévia;

É proibido o uso, dentro da área técnica, de celulares equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar vez que o local possui dados sensíveis de clientes/pacientes;

Relativo a Segurança perimetral ou física é limitada através de cadastro de entrada na portaria da empresa, sendo que o acesso as dependências da empresa visam proteger e mitigar possíveis ataques externos, quer seja por furto ou roubo, quer seja por roubo de informações por pessoas que adentraram maliciosamente na empresa.

Os servidores que armazenam sistemas utilizados pela empresa VALIDE SOLUÇÕES encontram-se em área protegida com acesso restrito na unidade matriz, localizada no bairro do Jaguaré, cidade de São Paulo.

4.2 Acesso à internet, rede de dados, sistemas/software e hardware pertencentes a empresa

As diretrizes e requisitos dos controles de acesso de aplicações e sistemas do ambiente de tecnologia, encontram-se determinadas abaixo:

- **Níveis de acesso a software:** todos os sistemas/software utilizados e adquiridos pela empresa VALIDE SOLUÇÕES devem possuir níveis de acesso aos diferentes usuários de modo que cada usuário tenha acesso somente as informações fundamentais a perfeita execução de seu trabalho;

- **Rede:** todos os departamentos da empresa VALIDE SOLUÇÕES possuem pasta própria e restrita na rede, cujo acesso é liberado pelo departamento de Tecnologia da Informação e a determinação

- de qual usuário pode ter acesso a determinada pasta ocorre através de solicitação da Diretoria da empresa e/ou do gestor da área;
  - **Pasta Pública**: a rede da empresa VALIDE SOLUÇÕES conta com uma pasta denominada pública que serve para interação entre os departamentos, ou seja, todos possuem acesso.
  - **Hardware**: o VALIDE SOLUÇÕES oferece a todos os seus colaboradores equipamentos suficientes a perfeita realização do seu trabalho, sendo, portanto, proibida a utilização de máquinas externas ao laboratório ou próprias dentro dos ambientes de trabalho da empresa, excetuando a esta determinação, as máquinas de assessores técnicos, consultores e auditores contratados pela empresa ou seus parceiros.

    O acesso aos computadores da empresa ocorrerá através de usuário e senha exclusivo (perfil) determinado pela **empresa**.

    Aos colaboradores e parceiros da empresa fica terminantemente proibido o salvamento de documentos em máquinas dos departamentos, todos os arquivos e documentos produzidos pelos diversos departamentos deverão ser salvos em pasta própria na rede da empresa;
  - **Dispositivos de gravação, portas USB, gravadores de CD e outros:** somente profissionais com autorização expressa pela empresa terão acesso a estas portas, os demais colaboradores terão acesso bloqueado;
  - **Portas VPN**: o acesso externo a rede da empresa VALIDE SOLUÇÕES ocorrerá tão somente através de Portas VPN, previamente solicitadas e autorizadas pela empresa de acordo com a POL-TI-002 POLÍTICA DE USO ACEITÁVEL DE VPN E SEGURANÇA DE REDE;
  - **Back-up da rede:** o back-up da rede do laboratório é realizado diariamente através de software específico para a função, sendo o armazenamento feito em duplicidade em cloud e servidor local;
  - **Antivírus:** a empresa oferece para todas as máquinas antivírus, sendo atualizado sempre que necessário de acordo com a POL-TI-003 - POLÍTICA DE ANTIVIRUS;
  - **Softwares**: as licenças Windows/office utilizadas são adquiridas juntamente aos computadores. Não sendo permitida, em nenhuma hipótese, instalação de Softwares piratas ou paralelos.

    Na necessidade de instalação de softwares e/ou aplicações no computador por algum motivo, Ex. Programa de Atualização CNES, sempre acontecerá pelos profissionais do departamento de TI, através de senha mestra, não sendo autorizado aos demais colaboradores instalação de nenhum software ou aplicativo;

- **E-mails**: a disponibilização de e-mails corporativos ocorre quando o perfil do cargo permitir e/ou acontecer a necessidade;

Os e-mails possuem protocolo de encriptação TLS para envio e recebimento de mensagens e as senhas dos usuários, podem ser trocadas trimestralmente ou quando ocorrer necessidade;

A empresa possui uma black-list de domínios que possam ser maliciosos que são bloqueados os recebimentos de e-mails;

E-mails pessoais não devem ser utilizados nas máquinas da empresa, exceto pessoas previamente autorizadas de acordo com a POL-TI-004 - POLÍTICA DE COMUNICAÇÃO ELETRÔNICA;

- **Criptografia de e-mails:** trata-se de recurso digital, disponibilizados nos e-mails corporativos que visam garantir a integridade e confidencialidade das informações através das mensagens de correio eletrônico;

  A criptografia é um processo padrão e automático dentro do servidor de e-mails.
- **Acesso a sites e redes sociais**: é proibido o acesso a sites desconhecidos, redes sociais, baixar e instalar programas de fontes de procedência duvidosa, utilizar dispositivos, como pendrives, e é terminantemente proibido: Acessar páginas de conteúdo pornográfico.

  É proibida a divulgação em redes sociais de informações internas da empresa, fotos e outros dados da corporação.

  Exceção: O Departamento de Marketing poderá acessar as redes sociais e/ou outros departamentos poderão utilizar desde que o uso tenha relação com a empresa e seus interesses.
- **Controle dos usuários**: o departamento de Tecnologia da Informação tem a função de controlar e disponibilizar o acesso dos usuários nos diversos sistemas utilizados pela empresa, sendo possível a transferência do controle de senhas a outros departamentos desde que solicitado pela diretoria;

  Cabe ao departamento de TI também monitorar o acesso a sites e conteúdo dos e-mails corporativos.
- **Rede wireless corporativa e acesso a internet:** cabe ao departamento de TI o gerenciamento, instalação, configuração, liberação de acesso e segurança para rede wireless e internet;

  Sendo imperioso observar que o uso do Wireless da empresa é exclusivo dos colaboradores da empresa nos dispositivos próprios da empresa, excetuando a esta determinação a disponibilização para assessores técnicos, consultores e auditores contratados pela empresa ou seus parceiros, desde que solicitado ao departamento de TI e previamente autorizado de acordo com POL-TI-005 - POLÍTICAS DE ACESSO A INTERNET.

  Aos usuários externos será concedido voucher de utilização com senha válida para uso da rede wireless por apenas um dia.

- **Cibersegurança:** cabe ao departamento de TI e/ou empresa contratada proteger os ativos de informação, computadores e servidores entre outros contra ameaças cibernéticas ou ataques maliciosos.

Para tanto, o departamento deverá:

a. Testar sistemas e redes em busca de vulnerabilidades desconhecidas e portas abertas para malwares que podem ser exploradas por cibercriminosos;
b. Fazer a gestão de cibersegurança na cloud, diminuindo os riscos da descentralização do armazenamento de dados;
c. Evitar ameaças de crimes cibernéticos e possíveis ataque aos sistemas e redes da empresa

5 CADEIA DE SUPRIMENTOS/ SUPPLY CHAIN

O Supply Chain da empresa VALIDE SOLUÇÕES é composto pelas áreas de Compras, Armazém e Transporte.

Considerando que a aquisição de suprimentos e sua disponibilização trata-se de estratégia da empresa, cabe ao departamento seleção, avaliação, classificação e reavaliação de fornecedores, obedecendo as normas pré-determinadas pela empresa.

A área é responsável pela autorização do acesso a empresa de carros, caminhões e/ou pessoas que possuam relacionamento com a empresa, para carga e descarga de produtos, insumos, além do transbordo de cargas biológicas.

6 TRABALHO REMOTO OU HOME OFFICE

A empresa não possui colaboradores 100% em home office, porém, em casos de necessidade, a empresa concederá equipamento para o trabalho, não devendo o profissional realizar suas funções em equipamento próprio.

O acesso aos dados/ rede e armazenamento devem ocorrer exclusivamente através de portas VPN criadas para este acesso que serão eliminadas no retorno do trabalho presencial, de acordo com a POL-TI-002 POLÍTICA DE USO ACEITÁVEL DE VPN E SEGURANÇA DE REDE;

Assim como os profissionais em trabalho presencial é vedado aos trabalhadores o uso pessoal dos equipamentos da empresa, excetuando os casos previamente aprovados.

As mensagens de e-mail devem ser realizadas pelo e-mail corporativo, garantida a criptografia de dados e conexão.

Treinamentos, palestras e/ou reuniões devem ser realizadas exclusivamente pela ferramenta Teams.

7 TRANSFERÊNCIA EXTERNA DE INFORMAÇÃO

A transferência de informação para contatos externos e/ou órgãos de governo (ex.: Notificação compulsória), somente é permitida para as previsões legais, devendo utilizar Firewall para filtrar e proteger as transferências de dados.

Poderá ocorrer transferência de dados também como forma de back-up em servidores próprios nacionais e/ou cloud.

Prevenção: compete a todas as áreas da empresa tomar medidas preventivas com o intuito de minimizar os riscos de invasão e vazamento de informações;

Desligamento de profissionais: no momento da demissão ou comunicação da demissão pelos demissionários, todas as senhas e acessos do colaborador deverão ser bloqueados;

Mudança de profissionais de departamento e/ou setor: modificar o nível de acesso do usuário de modo que o colaborador possua acesso adequado e pertinente as novas funções;

Gestão de mudanças de softwares ou aplicativos: quando a empresa decidir mudar os softwares e/ou aplicativos utilizados por quaisquer que sejam os motivos, o assunto deverá ser pauta de reunião da Alta Diretoria, que avaliará sobre as vantagens e desvantagens, deliberando se aprova ou não a mudança;

Cabe ao departamento de Tecnologia da Informação: conduzir junto aos departamentos envolvidos as regras gerais do processo de mudanças de software, visando assegurar a aplicação de métodos e controles que resultem no mínimo de impactos negativos, oriundos de mudanças mal planejadas e/ou executadas;

Gestão de vulnerabilidades técnicas: uma vez detectada possível vulnerabilidade, cabe ao departamento de TI tomar as medidas preventivas e/ou levar para a Alta Diretoria da empresa soluções capazes de minimizar ou solucionar o problema;

Gestão de auditorias: a empresa deverá passar por auditorias internas, através de auditores internos previamente treinados, minimamente trimestralmente ou quando a empresa sentir necessidade;

Auditorias externas: deverão ocorrer minimamente a cada oito meses, quando além da auditoria *in loco* o auditor deverá também avaliar os relatórios de auditoria interna;

Cabe aos auditores internos e externo: avaliar os riscos de comprometimento dos sistemas ou das informações, além de avaliar usuários, sistema, seus mecanismos e controles.

Conscientização: a empresa, através do Comitê de Segurança da Informação, deverá criar programa de conscientização e treinamento de segurança para colaboradores e prestadores de serviço e demais pessoas relacionadas a empresa;

Contratos: todos os contratos formalizados pela empresa a partir da vigência deste documento deverá conter cláusula exclusiva elaborada pelo Departamento Jurídico de atendimento as normas ISO 27.001:2013 e/ou Lei da LGPD.

Comunicação de vazamento: as áreas que identificarem algum tipo de vazamento da informação, por menor que seja, deverão comunicar ao DPO ou Membros do Comitê de Segurança da Informação ou Chefia direta, que deverá comunicar o assunto ao comitê de Segurança da Informação e Alta Diretoria, se necessário. Caso o incidente seja considerado grave o comitê poderá convocar reunião de forma extraordinária e com urgência, para deliberar sobre o fato, bem como realizar a abertura de não conformidades, processos administrativos e as medidas corretivas e preventivas cabíveis.

Intempéries da natureza: a empresa está localizada em local sem histórico de grandes enchentes, tremores, tufões e/ou outros tipos de ameças ambientais, por isso assume risco controlado de eventuais perdas, vez que todos os sistemas possuem back-ups. A empresa possui sistema de para-raios.

8 BOAS PRÁTICAS DE COMUNICAÇÃO NA EMPRESA

8.1 Assuntos internos tratados fora do ambiente da empresa

- Não é permitido tratativas de assuntos confidenciais, nomes e dados pessoais ou sensíveis de clientes e/ou empresa, **fora da empresa**;
- Quando inevitável a tratativa de assuntos da empresa **fora do ambiente** tomar máximo cuidado com locais públicos ou dentro da empresa quando estiver próximo a visitantes ou terceiros não envolvidos, seja ao telefone ou com algum colega ou mesmo fornecedor;

8.2 Autorizações

- Todo usuário deve ter uma identificação única, pessoal e intransferível, para acesso a rede e aos softwares utilizados pela empresa, qualificando-o como responsável por qualquer atividade desenvolvida sob sua identificação.
- O titular de usuário e senha de acesso a rede e softwares assume a responsabilidade quanto ao sigilo da sua senha pessoal;
- A distribuição de **senhas aos usuários** dos softwares deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário no primeiro acesso.

- As **autorizações** devem ser revistas, confirmadas e registradas continuamente;
- O responsável pela **autorização** ou confirmação da autorização deve ser claramente definido e registrado.

8.3 Segurança e acessos a informações

- Todo **acesso as informações** e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas as pessoas autorizadas;
- Os dados, as informações e os sistemas devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e **garantir a integridade**, sigilo e disponibilidade dos dados/ativos;
- A **segurança deve ser testada** regularmente e mantida atualizada;
- Os sistemas devem possuir **controle de acesso de modo** a assegurar o uso apenas a usuários ou processos autorizados;
- As necessidades de segurança devem ser identificadas para cada etapa do **ciclo de vida dos documentos** e dados tratados pela empresa;
- **Documentos** confidenciais não devem ficar **expostos com fácil acesso**, como por exemplo, sobre as mesas;

8.4 Informações sigilosas

- A empresa deve garantir que o acesso as **informações sigilosas** e/ou secretas, coorporativas ou cuja divulgação possa causar prejuízo a empresa, esteja disponível somente a um grupo seleto de usuários interessado e/ou envolvidos;
- **Informações sigilosas** e/ou secretas, coorporativas ou cuja divulgação possa causar prejuízo a empresa, só poderão ser utilizadas em equipamentos com controles adequados, que contenham identificação de usuário e senha;

8.5 Software, aplicativos e/ou programas

- Não executar **software, aplicativos e/ou programas** que tenham como finalidade a decodificação de senhas, monitoramento da rede, leitura de dados de terceiros, propagação de vírus, destruição parcial ou total de arquivos e/ou possa causar indisponibilidade de serviços;
- Não executar ou instalar **software, aplicativos e/ou programas** em equipamentos/ máquinas da empresa, bem como não armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados a rede coorporativa da empresa;

- Apenas pessoal autorizado de TI pode **instalar softwares** nas estações de trabalho dos usuários e devem utilizar apenas softwares licenciados pela empresa. Em caso de dúvidas, deverá consultar a área de TI através dos canais de suporte (Service Desk);
- A área de Infraestrutura de TI deverá estabelecer os controles, distribuição e instalação de softwares utilizados;

- É responsabilidade da área contratante em conjunto com o departamento de contratos de **terceiros/prestadores de serviço**, incluir no contrato da prestação de serviço cláusula declarando a responsabilidade da empresa terceira sobre todo e qualquer software instalado nos equipamentos, bem como atualização de antivírus e inspeção para verificação de existência de vírus;
- Qualquer **software** que, por necessidade do serviço, necessitar ser **instalado,** deverá ser comunicado a área de Suporte Técnico da TI, para que o mesmo possa ser instalado pelo Departamento de TI, homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente;
- A empresa respeita os **direitos autorais dos softwares** que usa e reconhece que deve pagar o justo valor por eles, coibindo e monitorando o eventual uso indevido de programas não licenciados.
- É terminantemente proibido o uso de **softwares ilegais** (sem licenciamento) na empresa;
- A gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer **software** sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software);
- Sobre os aplicativos de mensagem a empresa recomenda a utilização do aplicativo Kaizala;
- O uso de equipamentos de gravação como Pen-drives, CDS e outros não é permitida, devendo as portas serem trancadas pelo departamento de TI. A Alta diretoria e algumas gerências que necessitam de gravações poderão ter acesso as portas, desde que previamente definido pela diretoria.

8.6 Hardware

- As estações de trabalho/ **hardware**, incluindo equipamentos portáteis e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos;
- As estações de trabalho/ **hardware** pode ser identificadas na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do colaborador;

- O acesso a estação de trabalho/ **hardware** deverá ser encerrado no final do expediente, desligando o equipamento;
- Quando se ausentar da mesa, deverá bloquear a estação de trabalho/ **hardware** com senha. Esta ação aplica-se a todos os colaboradores com estações de trabalho, incluindo equipamentos portáteis;

8.7 Correio eletrônico/ e-mail

- Não enviar informações confidenciais para **e-mails** externos sem proteção. No mínimo, o arquivo deve contar com a proteção de criptografia;
- Arquivos de folhas de pagamento direcionados via **e-mail** também deverão ser encaminhadas através de e-mail criptografados;
- É vedado o uso de sistemas **webmail terceiro** (Gmail, Hotmail, Yahoo, etc). O uso do correio eletrônico para envio e recebimento de e-mail relativos à empresa deverá ocorrer exclusivamente através do correio eletrônico da empresa;
- É proibido o uso do **correio eletrônico** para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro;
- Evitar utilizar o **e-mail** da empresa para assuntos pessoais;
- **E-mail:** não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Em caso de dúvida, comunicar a área de TI;
- **E-mail:** não executar ou abrir links/endereços de e-mails suspeitos, como por exemplo bancos solicitando alguma informação pessoal. Verifique sempre se o e-mail ou o endereço do link são realmente de fontes conhecidas. Em caso de dúvida, comunicar a área de TI;
- Não utilizar o **e-mail** para enviar grande quantidade de mensagens (spam);
- Utilizar o **e-mail** para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isso diminui custo com impressão e aumenta a segurança e a agilidade na entrega e leitura do documento;
- O acesso externo ao **e-mail** corporativo por colaboradores em posições que possuam controle/reporte de jornada deve ser aprovado pelo diretor da área;

8.8 Equipamentos móveis

- Quando em deslocamento de carro, colocar **equipamentos móveis** como notebook no porta-malas ou em local não visível;
- Ao movimentar-se com **equipamentos móveis/** notebook, se possível, não utilize malas convencionais para notebook, utilizar mochilas e/ou malas discretas;
- Não coloque **equipamentos móveis/** notebook em carrinhos de aeroportos, nem despache junto com a bagagem;

- Em locais públicos (recepção de hotéis, restaurantes e aeroportos, dentre outros), mantenha **equipamentos móveis/** notebook próximo e sempre à vista, não se distanciando do equipamento;
- Evite utilizar **equipamentos móveis/** notebook em locais públicos;
- Nos hotéis, sempre que possível, guarde os **equipamentos móveis/** notebook no cofre do seu apartamento;
- Avalie se em pequenas viagens é realmente necessário levar **equipamentos móveis/** notebook;
- **Equipamentos móveis:** para tablets e celulares sempre utilize o bloqueio de tela com senha;
- **Equipamentos móveis:** não conecte em redes Wi-Fi desconhecidas, essas redes podem conter mecanismos para captura de dados do seu dispositivo;
- **Equipamentos móveis/** notebooks particulares para serem utilizados na rede corporativa, precisam ser avaliados e autorizados pela área de suporte de TI e só poderão ser utilizados se autorizado pela diretoria em caráter de exceção;

8.9 Impressão

- Documentos enviados para a **impressão** deverão ser retirados imediatamente;
- Não deixar documentos nas **impressoras**, em caso de erros e falhas solicitar auxílio/suporte da TI para que impressões posteriores não fiquem disponibilizadas em impressoras;
- Documentos confidenciais devem ser imediatamente recolhidos das **impressoras** pelo responsável após a sua impressão;

8.10 Uso de internet, acesso a redes sociais, sites de conteúdo adulto e outros

- A **internet** deve ser utilizada para fins coorporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas a empresa;
- O **acesso as páginas e web sites** é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdos impróprios e de relacionamentos;
- **Material sexualmente explícito** não pode ser acessado, exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa;
- O **uso da internet** para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários;
- O **acesso à internet** será monitorado pela área de TI;

- O uso do acesso via **VPN** deve ser restrito a colaboradores que sua posição permita acesso à rede coorporativa, estando fora das localidades de trabalho da empresa. Exceções deverão ser aprovadas pela diretoria da empresa.

9 VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta política, poderá ser aberto processo administrativo para denúncias de vazamento de informações e outros e/ou processo de não conformidade para casos de não cumprimento da norma, resultando em sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com advertências, suspensões, desligamento com justa causa e eventuais processos, se aplicáveis.

O colaborador infrator deverá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, a diretoria e a presidência, dependendo da gravidade e extensão da violação, sendo consignado/ garantido ao colaborador a ampla defesa e o contraditório.

Nos casos de abertura de processos disciplinares, será estabelecida comissão prévia de avaliação e por fim, emissão de relatório de apuração que será disponibilizado para a diretoria para providências cabíveis.

10 TRATAMENTO E AVALIAÇÃO DE NÃO CONFORMIDADES

Todos os requisitos legais, regulamentares e contratuais relevantes devem ser identificados, documentados e mantidos atualizados, garantindo a funcionabilidade do programa de segurança da informação. Quando violado estes termos, **deverá ser aberto e registrado procedimento de não conformidade.**

A empesa deve garantir o uso somente de softwares adquiridos, sendo proibido a utilização de qualquer programa "*pirata*" ou cópias não seguras e a confecção de documentos internos, uma vez consultados ou copiados partes de livros deverá constar a fonte. O uso de software não permitidos pela empresa é entendido como *falta grave* e deverá ser aberto procedimento administrativo bem como **abertura e tratamento de não conformidades.**

Os registros e cadastros devem ser protegidos contra a perda, eliminação, falsificação, acesso não autorizado, divulgação não autorizada, de acordo com os dispositivos legais e requisitos das normas, assegurando a proteção dos registros e cadastros, estando sujeitos a controle, conservação, manutenção e eliminação dentro dos prazos legais. Os dados pessoais identificáveis e dados sensíveis de clientes e/ou colaboradores são asseguradas pela empresa. Sendo mantidos e tratados em sistemas adequados a ISO 27.001:2013 e LGPD, e possuindo back-up de segurança em servidor e cloud sem trânsito internacional de informações. O vazamento de informações é entendido como falta grave e

deverá ser aberto procedimento administrativo bem como **abertura e tratamento de não conformidades.**

A empresa disponibiliza criptografia em seus e-mails e o uso de ferramentas de comunicação não permitidas é entendido como falta grave e deverá ser aberto procedimento administrativo bem como **abertura e tratamento de não conformidades.**

Os itens acima são alguns exemplos de não conformidades, porém, todo e qualquer desrespeito a lei, a norma e/ou ao programa de Segurança da Informação são não-conformidades que merecem ser avaliadas.

Chegando ao conhecimento do DPO e/ou comissão de segurança da informação, qualquer não conformidade ou violação ao presente documento, a comissão deverá abrir formalmente a não conformidade, estudar junto aos membros da comissão os aspectos da violação e as oportunidades de melhorais advindas do acontecimento, finalizar o relatório e submetê-lo a alta diretoria, bem como deixar registrado em sistema e/ou rede o relatório final de apuração.

11 AUDITORIAS INTERNAS, EXTERNAS E REVISÃO DO PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

A empresa deve regularmente, de acordo com o Manual de Segurança da Informação, realizar auditorias internas e externas, a fim de garantir a perfeita execução do programa de Segurança da Informação, bem como servir de tomada de decisão relativos aos resultados encontrados. Os gestores devem rever regularmente a conformidade dentro da sua área de responsabilidade quanto as normas e programa da segurança da informação.

A revisão e análise dos documentos relativos ao programa de Segurança da informação devem ser reavaliados minimamente na periodicidade prevista no Manual de Segurança da Informação, bem como quando ocorrerem alterações significativas ou sempre que necessário de forma independente e/ou em intervalos planejados.

12 CANAL DE COMUNICAÇÃO

E- mail: dpo@validesoluções .com.br