PCSIC
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA - INTERNA

PCSIC
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA - EXTERNA

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA GRUPO LAVORO			
MÊS / ANO	VERSÃO	CONFIDÊNCIALIDADE	DESCRIÇÃO
Novembro 2021	Versão 1.4 COMPLETA	Documento Público	Nº POL-SEG-001

Sumário

1 INTRODUÇÃO

Esta Política Corporativa de Segurança da Informação e Cibernética é mantida e divulgada pelo Grupo Lavoro Agro Holding ("Grupo Lavoro") para orientar seus colaboradores e prestadores de serviços sobre como proteger adequadamente as informações manipuladas no exercício de suas funções. Todas as informações do Grupo Lavoro, de seus clientes, colaboradores, prestadores de serviços, acionistas e demais partes interessadas devem ser obtidas, manipuladas, armazenadas e, eventualmente, destruídas conforme as determinações desta política.

As determinações aqui contidas refletem a visão, a missão e os valores do Grupo Lavoro, bem como o comprometimento do Comitê Executivo de Segurança da Informação com a proteção das informações da empresa ou sob sua guarda, conforme as determinações da legislação brasileira e as melhores práticas de mercado.

O objetivo desta política é garantir a continuidade do negócio através da mitigação dos riscos de segurança da informação, minimizando os impactos tangíveis e intangíveis, sendo a segurança da informação e a segurança dos sistemas de informação, elementos fundamentais para atingir os objetivos de governança alinhados com os objetivos corporativos e de negócios.

2 TERMOS E DEFINIÇÕES

Ativo: Qualquer recurso de processamento da informação digital ou físico que tenha valor para o Grupo Lavoro.

Código Móvel: Código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário. Exemplos de códigos móveis: activex, java, javascript, vbscript e macros embutidas em documentos do Microsoft Office.

Colaborador: Pessoa que esteja trabalhando em nome do Grupo Lavoro, como empregado, diretor, empregado temporário, empregado terceirizado, estagiário ou menor aprendiz.

Confidencialidade: Propriedade que garante que apenas pessoas autorizadas possuem acesso a informações sensíveis.

Contas de Serviço: São contas de acesso a sistemas e servidores, utilizadas apenas por sistemas. Não devem ser utilizadas por usuários comuns.

Disponibilidade: Propriedade que garante que informações sempre estarão disponíveis às pessoas autorizadas, sempre que estas solicitarem.

Dispositivos Móveis (Mobile): Dispositivos móveis são equipamentos portáteis que permitem sua operação de forma independente, podendo ser transportados e operados em movimento, normalmente com autonomia energética a baterias recarregáveis como notebook, smartphone, tablet, GPS, celular, entre outros.

Ferramenta de Acesso Remoto: Software que permite que os usuários controlem computadores remotos de suas máquinas locais. Poderá ser também entendido como ferramentas de produtividade que acessam o ambiente corporativo do Grupo Lavoro para realização de conferências, apresentações e demonstrações através da Internet.

Integridade: Propriedade que garante que informações não foram alteradas indevidamente ao longo de seu ciclo de vida.

Máquinas Virtuais (Virtual Machine): São computadores de software com a mesma funcionalidade que os computadores físicos. Assim como os computadores físicos, elas executam aplicativos, sistemas operacionais ou outros ambientes simulados.

Mobile Device Management (MDM): Sistema para Gerenciamento de Dispositivos Móveis.

Mídias Sociais: São canais online que permitem o relacionamento e compartilhamento de conteúdo entre usuários. Para que seja considerada uma mídia social, a plataforma, site ou aplicativo deve: 1. Promover a interação entre usuários 2. Permitir a divulgação descentralizada de conteúdo 3. Incentivar a participação colaborativa.

Acordo de Confidencialidade (Non-Disclosure Agreement - NDA): Modelo de acordo em que partes possam trocar informações confidenciais protegendo a relação de comunicação através de regras estritas de sigilo.
Serviços de computação em Nuvem (Cloud Computing): Fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet ("a nuvem") para oferecer inovações mais rápidas, recursos flexíveis e economias de escala.
Prestador de Serviço: Pessoa que esteja trabalhando em nome, para ou no Grupo Lavoro, ou que de alguma forma possa ter acesso a informações sensíveis, priveligiadas ou confidenciais, como, consultor, fornecedor, terceiro ou parceiro de negócio.
CLS: Centro Lavoro de Serviços.
Token: Aplicativo utilizado para autenticação através de senhas temporárias.
Transferência Segura de Arquivos: Definição utilizada para troca de arquivos ou informações entre partes, (colaboradores, prestadores, fornecedores ou parceiros), podendo ser feito o uso de criptografia ou ambiente seguro como rede privada virtual (Virtual Private Network).
Virtual Private Network (VPN): Rede privada virtual estabelecida entre clientes ou colaboradores fora do ambiente do Grupo Lavoro , permitindo desta forma, a realização de tarefas de forma remota.
Uniform Resource Locator (URL): Um URL em português "Localizador-Padrão de Recursos", é o endereço de um recurso (um arquivo, uma impressora etc.), disponível em uma rede; seja a Internet, ou uma rede corporativa, uma intranet. Uma URL tem a seguinte estrutura: "protocolo://máquina/caminho/recurso".

3 PREMISSAS

Os pilares da política de Segurança da Informação e Cibernética do Grupo Lavoro estão aderentes aos valores da Instituição e presentes no cumprimento da função de todos os colaboradores.
As suas premissas são:

- Proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados;
- Garantir a continuidade do processamento das informações críticas ao negócio;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual e atender às leis e normas que regulamentam as atividades do Grupo Lavoro em seu mercado de atuação;
- Determinar os mecanismos de gestão de riscos cibernéticos.

A informação é um dos principais bens da instituição. Assim, o Grupo Lavoro define a estratégia corporativa de segurança da Informação e cibernética para proteger a integridade, disponibilidade e confidencialidade da informação.
Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro digital do Grupo Lavoro.
Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde a coleta até o descarte.

4 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A nossa visão sobre Segurança da Informação e Cibernética está baseada nos seguintes princípios:

- **Confidencialidade** - Somente o Usuário da Informação, que esteja devidamente autorizado pelo Gestor da Informação, deve ter acesso às Informações respeitando os critérios de segregação de funções pré-definidos;
- **Integridade** - Garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo Gestor da Informação;

- **Disponibilidade** - Deve garantir que as Informações estejam sempre disponíveis para o Usuário da Informação;
- **Autenticidade** - Garante a identidade de quem está enviando a Informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem (irretratabilidade).

5 ABRANGÊNCIA EM SISTEMAS E ATIVOS COMPUTACIONAIS

As premissas definidas em política são aplicáveis a todos os ambientes computacionais de processamento de dados do Grupo Lavoro, estendendo, mas não se limitando a todos os servidores, bases de dados, sistemas operacionais, hardware, software, dispositivos de redes, telefonia, dispositivos móveis, além de ambientes de terceiros que de forma física ou lógica estejam integrados ou conectados nos ambientes do Grupo Lavoro e seu parque tecnológico.

O Grupo Lavoro pauta suas ações em boas práticas do mercado nacional e internacional, são elas:

- ISO 27701 – Gestão da segurança da Informação;
- ISO 27002 – Políticas para segurança da informação;
- NIST – Cyber Security Framework;
- CIS – Center for Internet Security;
- Resolução BACEN 4.658/18.

6 DIRETRIZES

Todas as políticas de segurança da informação devem estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

As políticas de segurança da informação são revisadas anualmente pelo Grupo Lavoro com aplicação no Brasil e no exterior.

A inclusão de diretrizes ou exceções por requisito regulatório e a publicação nas unidades do exterior, serão identificadas pelo responsável por segurança da informação da unidade, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pela Diretoria de Segurança Corporativa ou Diretoria de TI equivalente designada.

A adesão à essa Política e eventuais desvios, no Brasil e nas unidades no exterior, são reportados periodicamente pela Diretoria de Segurança Corporativa aos Comitê Executivo, Comitê de Auditoria e demais comitês de risco. A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente.

7 PRIVACIDADE DE DADOS

O Grupo Lavoro preza pelo sigilo das informações sob a sua guarda, adotando as melhores práticas de mercado, empregando controles de segurança da informação para garantir a privacidade conforme a Constituição Federal, a legislação e a regulamentação aplicáveis a sua área de atuação.

Portanto fica vedada a qualquer colaborador ou prestador de serviço prover qualquer informação sobre clientes, colaboradores, ou prestadores de serviço do Grupo Lavoro para terceiros, sendo considerado tal ato como crime de extração de ativo de dados.

8 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Grupo Lavoro define o Comitê de Segurança da Informação como a maior autoridade para avaliação de políticas, padrões e procedimentos no que tange à Segurança da Informação.

8.1 REPRESENTAÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Comitê de Segurança da Informação é multidisciplinar, sendo composto por representantes dos seguintes departamentos:

- Jurídico e Compliance;
- Finanças;
- Recursos Humanos;
- Marketing;
- Controles Internos; e
- Tecnologia da Informação.

Havendo a necessidade, representantes de outras áreas podem ser convidados a participar de reuniões do Comitê de Segurança da Informação.

8.2 ATIVIDADES DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

1. Avaliar as Políticas de Segurança da Informação, para posterior aprovação da Presidência.
2. Identificar e atribuir responsabilidades com relação à Segurança da Informação;
3. Avaliar e monitorar o nível de Segurança da Informação do Grupo Lavoro e indicar possíveis auditorias nos processos descritos nesta política;
4. Monitorar alterações que possam afetar a Segurança da Informação e, caso necessário, aprovar as iniciativas de melhoria nos níveis de Maturidade em Segurança Cibernética;
5. Definir regras sobre situações não previstas em procedimento interno do Grupo Lavoro

9 ABRANGÊNCIA E RESPONSABILIDADES

Todos os envolvidos que utilizam ou possuem acesso à informação ou aos recursos de processamento do Grupo Lavoro ou sob sua custódia, sejam colaboradores ou prestadores de serviços, devem garantir que as práticas definidas na Política de Segurança da Informação e Cibernética sejam aplicadas e seguidas continuamente. Para isto, todos os colaboradores e prestadores de serviço devem assinar os termos de confidencialidade e de responsabilidade.

O Grupo Lavoro possui um NDA padrão que deve ser firmado sempre antes que qualquer informação seja trocada entre um Colaborador e um Prestador de Serviço. A área de Contratos é responsável por produzir, gerenciar e armazenar os NDA´s firmados pelo Grupo Lavoro.

Aqueles empregados que, uma vez cientes, violem as regras de segurança, estarão sujeitos a ação disciplinar interna conforme Política de Consequências do Programa de Integridade do Grupo Lavoro, sem prejuízo das demais sanções e responsabilidades civis, criminais e trabalhistas aplicáveis.

No que se refere aos prestadores de serviços a violação das regras da Política de Segurança da Informação e Cibernética serão tratadas conforme acordado em contrato e lei aplicável.

9.1 CATEGORIAS DE RESPONSABILIDADES

Para operacionalizar o controle dos direitos e deveres relativos à Segurança da Informação, o Grupo Lavoro adota o sistema de categorias de responsabilidades.

9.1.1 Responsável

Os Responsáveis pelas Informações são os Responsáveis pelas Áreas, Diretores ou seus Representantes. São, em suma, as pessoas com a responsabilidade pela aquisição, criação, manutenção e descarte das informações da empresa.

Os Responsáveis avaliam o risco, definem a classificação da informação, definem os controles de segurança e quais pessoas podem ter acesso à informação. É também atribuição do Responsável aprovar a forma com que as informações serão utilizadas e zelar por ela.

Toda a aplicação, sistema ou informação crítica, obrigatoriamente deve ter um Responsável designado. Os Responsáveis devem definir a classificação de sensibilidade e a quais usuários o acesso será concedido.

9.1.2 Depositário

Os Depositários têm a posse física ou lógica da informação. São responsáveis pela guarda da informação, incluindo a implementação de sistemas de controle de acesso e a manutenção de cópias de segurança. Também são responsabilidades dos Depositários a implementação, a operação e a manutenção das medidas de segurança definidas pelos Responsáveis.
Sempre que uma informação é mantida em um equipamento de propriedade do Grupo Lavoro, o usuário necessariamente será também o Depositário. Portanto, cada sistema ou aplicação, obrigatoriamente, deve ter um ou mais Depositários designados.
Os Administradores de Rede ou Sistema Corporativos são claramente Depositários, bem como os Administradores de Sistemas Locais.

9.1.3 Usuário

Os Usuários devem se familiarizar e seguir todos os itens da Política de Segurança da Informação e Cibernética. Dúvidas sobre a manipulação apropriada de um tipo específico de informação devem ser dirigidas ao Depositário do Ativo ou ao Responsável pelo Ativo.
Casos duvidosos ou omissos devem ser avaliados pela área de Segurança da Informação, para que sejam tomadas as devidas providências.

10 MANUTENÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação deve ser revisada a cada 12 meses. O Comitê de Segurança da Informação pode, no entanto, iniciar o processo de revisão a qualquer momento. A decisão de revisar a Política de Segurança da Informação pode ser tomada com base em critérios próprios ou a partir de um dos seguintes acontecimentos:

1. Incidentes de segurança considerados significativos;
2. Novas vulnerabilidades identificadas;
3. Vulnerabilidades identificadas em uma Análise de Risco;
4. Alteração ou publicação de legislação aplicável à segurança de dados;
5. Mudanças na estrutura técnica ou organizacional do Grupo Lavoro.

Uma revisão da Política de Segurança da Informação deve incluir no mínimo os seguintes itens:

1. A eficiência e eficácia da Política de Segurança da Informação. Esta avaliação deve tomar por base os incidentes registrados: o número, tipo, o impacto causado etc.;
2. O custo e os impactos dos controles na eficiência e lucratividade do Grupo Lavoro;
3. Efeitos positivos ou negativos de mudanças tecnológicas.

Toda revisão deve ser analisada pelo Comitê de Segurança da Informação e formalmente registrada. As modificações, bem como o controle de versão da Política de Segurança da Informação devem ser cuidadosamente observados.

11 POLÍTICAS ESPECÍFICAS

A Política de Segurança da Informação é composta pelas Diretrizes e as seguintes políticas específicas:

1. Política de Classificação de Informações;
2. Política de Controle de Acesso e Autenticação;
3. Política de Uso de Equipamentos e Recursos de TI;
4. Política de Uso de Portáteis e Acesso Remoto;
5. Política de Acesso à Internet;

6. Política de Uso de Correio Eletrônico;
7. Política de Segurança em Recursos Humanos;
8. Política de Segurança Física e do Ambiente;
9. Política de Operações e Gerências de Sistemas;
10. Política de Desenvolvimento e Implantação de Sistemas;
11. Política de Gerência de Incidentes de Segurança;
12. Política de Conformidade;
13. Política de Continuidade de Negócios.

11.1 POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÕES

11.1.1 Inventário de Ativos de Informação

Os ativos de informação que sejam importantes para a empresa devem ser cadastrados e mantidos em um inventário.

Nesse cadastro devem constar informações detalhadas sobre o ativo, o nome do seu Responsável, Depositário e o seu nível de confidencialidade.

11.1.2 Informações Sensíveis

Informação sensível é toda a informação classificada como Secreta ou Confidencial. Mesmo que a informação não esteja escrita ou gravada em meio eletrônico ela pode e deve ser classificada. O procedimento padrão deve ser informar aos interlocutores previamente sobre a criticidade da informação. Por exemplo, no início de uma reunião os participantes devem ser informados que será tratado um assunto secreto, que deve ser mantido em sigilo.

11.1.3 Dados Pessoais

Dados Pessoais: Quaisquer informações relativas a uma pessoa física identificada ou identificável ("titular dos dados") que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dados Pessoais Sensíveis: Dados pessoais que são, por sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais merecem proteção específica, pois o contexto de seu processamento poderia criar riscos significativos aos direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou associação sindical, dados genéticos, dados biométricos com o propósito de identificar exclusivamente uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física.

11.1.4 Classificação da Informação

É atribuição do Responsável efetuar a classificação da informação de acordo com esta política. O Responsável deve certificar-se que possui todos os elementos para determinar o nível adequado de classificação. Caso contrário deve solicitar auxílio à equipe de Segurança da Informação (IT Security).

O Grupo Lavoro utiliza os seguintes níveis de confidencialidade para classificação das informações:

1. **Secreta**: Esta classificação se aplica a informações cujo acesso deve ser muito restrito, mesmo dentro do Grupo Lavoro. Sua revelação sem autorização pode prejudicar seriamente o Grupo Lavoro e/ou seus clientes. Normalmente informações secretas envolvem privacidade da companhia, estratégias corporativas, informações sensíveis de interesse de concorrentes, segredo em negociações, especificações, listas de clientes e dados estatísticos.

2. **Confidencial**: Esta classificação se aplica a informações cujo acesso deve ser restrito, mesmo dentro do Grupo Lavoro. Sua revelação sem autorização causaria prejuízos ao Grupo Lavoro e/ou a seus clientes. Informações privadas dos usuários, contratos, avaliações de mercado e senhas de acesso são alguns exemplos de informação confidencial.
3. **Uso Interno**: Esta classificação se aplica a toda informação que não se ajusta claramente nas anteriores. Entretanto sua revelação poderia prejudicar ou causar constrangimentos ao Grupo Lavoro. Exemplos incluem a lista telefônica interna, materiais de treinamento e manuais técnicos entre outros.
4. **Pública**: Esta classificação se aplica a toda informação que foi explicitamente aprovada pelo Responsável e pela Área de Comunicação Corporativa para liberação irrestrita. Exemplos desse tipo de informação incluem: anúncios de produtos ou serviços, boletins de imprensa, catálogos de produtos ou outros materiais de divulgação. Somente a área de Comunicação Corporativa do Grupo Lavoro está autorizada a fornecer conteúdo para o domínio público.

11.1.5 Identificação da Informação

A informação classificada deve ser etiquetada (marcada, rotulada) com a designação de classificação apropriada. Tais marcas têm que aparecer em todas as manifestações da informação (documento eletrônico, tela de computador, impressões, mídias removíveis etc.).
Toda informação sem rótulo, com exceção da classificada como pública: anúncios de produtos ou serviços, boletins de imprensa, catálogos de produtos ou outros materiais de divulgação, é considerada como “Uso Interno”.

11.1.6 Reclassificação da Informação

Sempre que o Responsável identificar que é necessário, deve-se proceder com a reclassificação da informação. Quando efetuar uma reclassificação, o Responsável deve comunicar adequadamente todas as partes interessadas.

11.1.7 Destruição da Informação

As informações, quando perdem sua utilidade ou valor, devem ser destruídas. O responsável tem poder para decidir sobre a destruição da informação.
Informações sensíveis impressas ou gravadas em mídias digitais devem ser fragmentadas ou inutilizadas ao serem descartadas para impedir que elas sejam reproduzidas.

Os propósitos, métodos, limitação de armazenamento, período de retenção de dados pessoais e a destruição devem ser consistentes com as informações contidas no Aviso de Privacidade. A Companhia deve manter a precisão, integridade, confidencialidade e relevância dos dados pessoais com base no propósito de processamento. Mecanismos de segurança adequados projetados para proteger dados pessoais devem ser usados para evitar que dados pessoais sejam roubados, mal utilizados ou abusados e evitem violações de dados pessoais. A TI é responsável pelo cumprimento dos requisitos listados nesta seção. Segundo o artigo 12 e 34 do código de defesa do Consumidor, o prazo de armazenamento dos dados cadastrais deve ser mantido por até 5 anos após o término da relação. Equipamentos e mídia de armazenamento móvel, devem ser apagados utilizando uma ferramenta de limpeza profunda, a qual, realize no mínimo 7 passos de sobrescrita complexa. Já os colaboradores que utilizam documentos individuais em papel, são responsáveis por destruí-los utilizando trituradores de papel. Em relação ao artigo 15 do Marco Civil da Internet, os dados de identificação digital devem permanecer por um período de até 6 meses.

O único impedimento à decisão de destruição da informação é a necessidade de retenção para atender requisitos legais, os quais devem ser verificados junto ao Departamento Jurídico.
Os registros de eliminação/destruição devem ser mantidos para todos os dados classificados como "Restrito" e "Confidencial". Os registros devem incluir as seguintes informações: informações sobre a mídia, data de eliminação/destruição, método de eliminação/destruição, pessoa que realizou o processo.
Todas as informações classificadas como "Confidenciais" devem ser apagadas/destruídas na presença de uma comissão composta por pessoas autorizadas a acessar as informações em questão.

11.1.8 Armazenamento da Informação
O armazenamento da informação deve ser feito com os controles de segurança adequados ao nível de confidencialidade da informação.
Os dados coletados serão armazenados em servidores localizados nos servidores de nuvem da Oracle Cloud Infrastructure, Google Cloud Platform e no Office 365 (Exchange Online, OneDrive for Business e SharePoint Online). O ambiente do Grupo Lavoro utiliza os meios razoáveis de mercado e legalmente requeridos para preservar a privacidade dos dados coletados. Avaliar métodos e ferramentas existentes como criptografia, anonimização, minimização de privilégio e autorização de acessos físicos ao datacenter.
Caso, para qualquer categoria de documento não especificamente definido em outros lugares desta Política e, a menos que de outra forma seja exigido de forma diferente pela lei aplicável, o período de retenção necessário para tal documento será considerado 5 anos a partir da data de criação do documento.
O Oficial de Proteção de dados (DPO) definirá o período para o qual os documentos e registros devem ser retidos.
Demais recomendações sobre este assunto podem ser encontrado no item 11.3.18.

11.1.9 Transmissão da Informação
Definições:
Exportador: O controlador que transfere os dados pessoais.
Importador: O processador/operador estabelecido em um país terceiro que concorda em receber do exportador, dados pessoais destinados ao processamento/operação em nome do exportador de dados após a transferência, de acordo com as instruções e termos das leis aplicáveis do país do exportador.
Antes da transferência ocorrer, o importador deverá informar ao controlador/exportador todas as políticas, leis, meios e tecnologias aplicáveis que garantam a proteção aos dados pessoais.
Após o envio de toda a documentação enviada pelo importador ao exportador, ela terá um prazo mínimo para análise pela equipe do exportador. Após sua aprovação, um contrato será enviado a fim de especificar todos os dados necessários, as finalidades e operações que serão realizadas. Este documento deverá ser aprovado pela ANPD antes do início da transferência dos dados.
Caso o operador/importador não possa fornecer tal conformidade, deverá informar imediatamente ao exportador sua incapacidade de cumprimento, e neste caso, o controlador/exportador poderá suspender ou rescindir o contrato imediatamente.
As informações devem ser transmitidas através de meios que implantam os controles de segurança adequados ao nível de confidencialidade das informações.
Para a transmissão de arquivos com fornecedores e parceiros, deve ser utilizado o Guia para “Transferência Segura”.
Para transmissão constante de arquivos, deve ser estabelecida uma conexão VPN com o fornecedor, mais informações devem ser solicitadas pelo responsável imediato do CSL, ou através de abertura de chamado contendo a descrição “Solicitação de Acesso à VPN entre Empresas”.

Não deve ser utilizado nenhum tipo de ferramenta de compartilhamento de arquivos na “nuvem” para transmissão de arquivos pertinentes ao Grupo Lavoro .

11.2 POLÍTICA DE CONTROLE DE ACESSO E AUTENTICAÇÃO

11.2.1 Registro do Usuário

Todo usuário que acessa o ambiente de Tecnologia do Grupo Lavoro deve ser identificado lógica e unicamente através de sua conta (“login” e senha) de uso exclusivo. As senhas de acesso são confidenciais e individuais e sua revelação a outros ou permitir o seu uso por outros é proibida conforme previsão do Código de Conduta e Ética do Grupo Lavoro.

11.2.2 Cadastro, Alteração e Exclusão de Cargos ou Funções

É responsabilidade da TI implantar e controlar procedimentos de aprovação, criação, bloqueio e exclusão dos usuários nos sistemas. Quando tecnicamente viável, as informações dos colaboradores, contidas na base de dados da área de Recursos Humanos, devem ser utilizadas como fonte para o cadastro do colaborador nos demais sistemas.

Sempre que o Departamento de Recursos Humanos ou Gestor da Pessoa, registrarem e informarem a alteração do cargo/função de um colaborador ou prestador de serviço, os seus direitos de acesso às informações devem ser revisados pelos responsáveis de perfis dos acessos concedidos ao colaborador ou prestador de serviço. É de extrema importância que o departamento de recursos humanos ou o gestor do colaborador realize a abertura de um chamado com no mínimo 4 horas de antecedência para programação da atividade.

Os colaboradores que forem afastados ou desligados, e os prestadores de serviços que encerrem o contrato com o Grupo Lavoro, devem ter sua conta bloqueada em todos os sistemas. Adicionalmente as contas que não forem utilizadas com período superior a 45 dias devem ser bloqueadas.

As contas de colaboradores ou prestadores de serviços que estiverem bloqueadas por mais de 90 dias devem ser excluídas/desabilitadas dos sistemas. Caso necessário o acesso, uma nova solicitação deverá ser realizada via abertura de chamado via CSL.

11.2.3 Controle de Privilégios

É responsabilidade da TI controlar os direitos de acesso de contas de sistemas corporativos, como “super usuário”, administrador ou quaisquer outras denominações que signifiquem poderes adicionais para instalar, alterar ou apagar informações. Os controles devem observar, pelo menos:

1. Utilização de um usuário diferente do normal, quando este estiver executando tarefas de “Super Usuário”;
2. Clara identificação de quais usuários têm acesso às “contas privilegiadas”;
3. Registro de uso das contas, com verificação periódica.

11.2.4 Troca de Senha de Acesso Privilegiado

As senhas administrativas devem ser trocadas periodicamente respeitando requisitos de complexidade mínimos e o tempo máximo de 90 dias.

Em caso de exceções, é necessária a assinatura de termo de não conformidade com a política do colaborador, assinatura do gestor responsável da área/departamento e do gestor de TI.

11.2.5 Privilégios em Equipamentos Específicos

É responsabilidade da TI configurar os direitos dos usuários de forma que estes possuam direitos mínimos de acesso na estação de trabalho, servidores e demais equipamentos, mas suficientes para a execução de suas tarefas.

Para casos específicos, onde os requisitos de negócio ou dificuldade técnica tornem obrigatória a concessão de direitos adicionais, no mínimo os seguintes controles compensatórios devem ser implementados:

1. Registro do identificador do usuário com poderes adicionais;
2. Registro do identificador do equipamento, ou equipamentos, onde os direitos foram concedidos;
3. Justificativa da concessão de tal acesso;
4. Assinatura do colaborador se responsabilizando pelas atividades que necessitam de superpoderes administrativos.

11.2.6 Armazenamento de Senhas de Acesso Privilegiado

As senhas das contas administrativas deverão ser armazenadas em guarda compartilhada, cofre ou sistema de criptografia.

11.2.7 Acesso de Administradores aos Sistemas

Os administradores de sistema devem efetuar acesso somente a informações para uso de suas atividades. É terminantemente proibido aos administradores acessar dados privados de quaisquer outras pessoas, departamentos, sejam colaboradores, clientes ou prestadores de serviços, sem justificativa.

Os dados acessados pelos administradores de sistemas não devem ser compartilhados com pessoas não autorizadas.

Em casos específicos, os Administradores de Sistema devem trabalhar em conjunto com a área de Ouvidoria/Canal de Denúncia, única autorizada a efetuar investigações e solicitar registros e acessos a informações.

11.2.8 Regras para Criação de Contas

Na composição dos nomes de contas na rede “logins”, deverão ser atendidos os seguintes critérios básicos:

1. O sistema de credenciamento de acesso aos sistemas do Grupo Lavoro é através do AD (Active Directory da Microsoft).
2. A regra de criação de contas segue os parâmetros especificados no item 11.6.3 (Regras para Criação de Contas de Email) desta política.
3. Caso algum sistema não possua integração com o AD, ainda assim deverá respeitar as mesmas regras descritas no item 11.6.3 desta política.

11.2.9 Configuração de Senhas de Acesso

É responsabilidade da TI, sempre que tecnicamente viável, parametrizar os sistemas com, no mínimo, as seguintes regras:

1. Utilização no mínimo de 11 caracteres;
2. Utilização de caracteres alfanuméricos e caracteres especiais;
3. Não permitir a troca antes de um (01) dia;
4. Exigir a troca a cada 90 dias;
5. Não permitir o uso das últimas 06 senhas;
6. Exigir a troca da senha padrão no primeiro acesso do usuário;
7. Bloqueio do acesso após três tentativas malsucedidas (deverá ser aberto chamado via CSL para orientação e desbloqueio da conta afetada).

A TI, para casos específicos e visando proteger os ativos do Grupo Lavoro pode definir requisitos mais restritivos dos que foram definidos acima.

Caso o sistema ou aplicação não suporte todos os requisitos citados acima, ele será tratado como exceção.

11.2.10 Fornecimento de Senhas de Acesso

As senhas não serão fornecidas por telefone. Em casos de exceção, é permitido o envio da senha para o e-mail particular do colaborador, cadastrado/atualizado pessoalmente, com a validação dos demais dados do solicitante.

11.2.11 Armazenamento de Senha

As senhas não devem ser guardadas de forma legível em arquivos, bases de dados, macros de software, chaves de função, terminais, anotadas em papel, ou em outros locais, nos quais, pessoas sem autorização possam ter acesso.

11.2.12 Senhas Padrão

É responsabilidade da TI alterar a senha de equipamentos ou sistemas que utilizem uma senha padrão, no momento de sua instalação ou recebimento, antes de sua entrada em atividade.

11.2.13 Acesso Administrativo Padrão

Contas de acesso padrão com privilégios especiais, como por exemplo, usuários “root” e “administrador”, não devem ser utilizados nas atividades do dia a dia. A senha dessas contas deve ficar sob responsabilidade do gestor de TI. Para atividades do dia a dia uma conta com poderes de root/administrador deve ser criada para cada administrador do ambiente de TI e se possível limitada de acordo com a necessidade. Isso permitirá a rastreabilidade das ações executas.

11.2.14 Verificação de Direitos

É dever dos responsáveis por perfis de ativos de informação revisar os direitos de acesso concedidos aos usuários, no mínimo, a cada 06 meses. Um esforço conjunto do Responsável, TI e Recursos Humanos deve ser efetuado para revogar os direitos redundantes ou desnecessários.
Usuários com privilégios especiais de acesso a sistemas críticos devem ter seus direitos revisados a cada 03 meses. Como privilégios especiais se entendem funções de administradores ou operadores com direito de escrita ou alteração nos sistemas.

11.2.15 Privilégio mínimo

Os usuários devem receber apenas os direitos necessários para a execução de suas atividades.

11.2.16 Armazenamento em nuvem – Cloud Drive

O único sistema/software de armazenamento e sincronização de arquivos autorizado pelo Grupo Lavoro é o OneDrive.

11.2.17 Perfis de Uso e Direitos

Devem ser criados perfis, acessos e grupos de usuários com a finalidade de se reduzirem riscos relacionados ao gerenciamento de acessos. Como grupo ou perfis entendem-se vários usuários que estão sob as mesmas regras e podem ser gerenciados em conjunto.

Para as aplicações que não permitem níveis de segregação, as atividades dos usuários devem ser registradas pela aplicação e posteriormente devem ser verificadas pelo gestor do usuário.

11.2.18 Direitos

Os direitos de acesso devem ser cadastrados nos grupos ou perfis de acordo com as necessidades de negócio do Grupo Lavoro. Em ambos os casos os direitos devem ser aprovados pelo gestor da pessoa e posteriormente pelo responsável do perfil e ou ativo, o qual deve ser um empregado do Grupo Lavoro e em cargo de confiança. O gestor da pessoa e o responsável pelo perfil ou ativo devem efetuar uma análise se a pessoa realmente necessita do acesso, autorizando somente o necessário.

11.2.19 Responsável pelo Grupo ou Perfil de Acesso

Todo grupo de usuário ou perfil, deve ter um Responsável nomeado. As funções do Responsável pelo grupo ou perfil são:

1. Determinar os direitos dos usuários;
2. Aprovar o cadastro de novos usuários;
3. Verificar o correto uso dos direitos;
4. Revisar periodicamente a validade dos direitos concedidos;
5. Revogar os direitos do usuário quando não mais necessário.

11.2.20 Segregação de Tarefas

Os gestores das áreas devem efetuar a segregação de tarefas para impedir modificações e acessos não autorizados às informações.

À TI cabe implementar as segregações de acordo com as orientações das áreas de negócio.

Para as aplicações que não permitem níveis de segregação, as atividades dos usuários devem ser registradas pela aplicação e posteriormente devem ser verificadas pelo gestor do usuário.

11.2.21 Bloqueio de Usuários Inativos

É responsabilidade da TI implementar um procedimento de bloqueio dos usuários que não acessam os sistemas há mais de 45 dias. Uma avaliação posterior por parte do Responsável pelo ativo definirá se os usuários bloqueados devem ser definitivamente excluídos/desabilitados.

11.2.22 Limite de Tempo de Sessão

Quando o sistema permitir deve ser configurado para desconectar a sessão do usuário após 30 minutos de inatividade para diminuir a possibilidade de acesso não autorizado.

11.2.23 Acesso de Fornecedores

O acesso de fornecedores a sistemas e informações do Grupo Lavoro deve ser devidamente controlado, os requisitos de segurança estabelecidos na Política de Controle de Acesso e Autenticação devem ser verificados antes que a concessão seja efetuada.

Os fornecedores que tiverem acesso a sistemas e informações do Grupo Lavoro devem declarar estar cientes e aderir formalmente a esta política, bem como realizar a assinatura do NDA.

11.3 POLÍTICA DE USO DE EQUIPAMENTOS E RECURSOS DE TI

11.3.1 Uso Autorizado

Os equipamentos e sistemas de propriedade do Grupo Lavoro devem ser usados para atividades profissionais. Os usuários não devem utilizar-se dos equipamentos ou sistemas de informação de maneira que a sua produtividade ou de outros usuários seja prejudicada.
O uso pessoal ocasional é permissível desde que:

1. Seja formalmente autorizado pelo gestor da área;
2. Não interfira com a produtividade do usuário.

Todo acesso aos recursos do Grupo Lavoro deve ser formalmente autorizados.

11.3.2 Uso Proibido

Os usuários não devem tentar burlar os controles técnicos existentes ou obterem acesso a qualquer informação que não tenha sido explicitamente autorizada ou que façam parte das suas atividades na empresa. Portanto, é proibido:

1. Efetuar varreduras de rede, de portas ou de segurança (sniffing de rede, port scanning e security scanning);
2. Tentar ou utilizar ferramentas para a enumeração/descoberta de redes, serviços, contas de serviços e usuários;
3. Efetuar monitoramento de rede para interceptar dados não direcionados ao computador do usuário;
4. Tentar ou burlar a segurança, autenticação de qualquer computador, rede ou conta de acesso;
5. Utilizar programas ou comando para sobrepor os controles existentes/escalação de privilégios ou interferir na usabilidade de outros usuários;

11.3.3 Uso particular ou de terceiros

Não é permitida a conexão de qualquer dispositivo pessoal ou de terceiros (computador, notebook, hub, switch, smartphone, tablet etc.) nos equipamentos ou na rede do Grupo Lavoro sem a autorização da equipe de Segurança da Informação (IT Security).
Em caso de necessidade de conectar a estação ou notebook na rede do Grupo Lavoro, o equipamento deverá ser configurado nos padrões do Grupo Lavoro de acordo com o procedimento realizado pela equipe de suporte ao usuário.
A solicitação de adequação de segurança deverá ser feita através da abertura de ticket de suporte com a área de Infraestrutura, e o solicitante assinará contrato digital contendo termo de ciência da adequação do equipamento, termo de responsabilidade de uso no ambiente Grupo Lavoro e termo de conhecimento das regras contidas neste manual de Políticas Corporativas de Segurança da Informação e Cibernética.
Equipamentos particulares ou de terceiros deverão se conectar primariamente na rede visitantes, mediante solicitação de acesso, identificador de acesso e liberação em sistema de controle de acesso.

11.3.4 Softwares/Sistemas

A utilização de sistemas ou softwares disponibilizados pelo Grupo Lavoro não deverão ser instalados/configurados em equipamentos particulares ou de terceiros.

11.3.5 Mudanças de Configuração

O Grupo Lavoro fornece equipamentos pré-configurados com os padrões da empresa para os usuários. O usuário não tem permissão para mudar a configuração do sistema operacional, nem de instalar novos programas. Da mesma forma, é proibido realizar alterações na configuração de hardware nem conectar periféricos ou outros equipamentos que não tenham sido fornecidos pela empresa.

Também não é permitido o compartilhamento de pastas locais em estações de trabalho e notebooks, devendo ser utilizados os compartilhamentos de rede disponibilizados pela empresa. Não é permitido executar qualquer tipo de sistema/software conhecidos como portable. Além disso, a inicialização do computador/desktop/notebook a partir de uma midia física, também conhecida como inicialização por pendrive, bootable pendrive, software inicializável, live cd entre outras, não é permitida.
Quaisquer mudanças de configuração que sejam necessárias devem ser solicitadas ao Suporte de Infraestrutura de TI via Ticket de chamado.

11.3.6 Sistema Antivírus
Todos os computadores devem ter sistema de antivírus instalado e ativo conforme os procedimentos da empresa. É proibido desativar/desinstalar o sistema de antivírus.

11.3.7 Erradicação de Vírus
Os vírus podem ser complexos e sofisticados, assim os usuários não devem tentar erradicá-los sem ajuda de um especialista. Se os usuários suspeitarem da infecção por um vírus, por favor, não desliguem o computador, apenas remova o cabo de rede ou desconecte-se da wi-fi e acionem imediatamente a equipe de segurança/resposta a incidentes do Grupo Lavoro. Nossa equipe irá orientá-lo de como proceder.

11.3.8 Login e Senha
Todo o acesso a equipamentos e sistemas do Grupo Lavoro deve exigir a utilização de um identificador de usuário (Login) e a validação necessária mediante senha, conforme a Política de Controle de Acessos e os procedimentos da empresa. O compartilhamento de usuário e senha é proibido. Para usuários com permissões adicionais ou de administradores, será implementado o sistema de multifator de autenticação, para aprimoramento da segurança.

11.3.9 Proteção do Equipamento
Todos os PCs, notebooks e estações de trabalho devem estar seguros por protetor de tela com senha ativada automaticamente para 5 minutos ou menos, ou logoff/bloqueio (para usuários Windows, tecla Windows + L) quando a estação não estiver em uso. Estações de trabalhos – PC's, onde a segurança física esteja aquém do mínimo exigido, deverão possuir criptografia, assim como os notebooks/laptops que a empresa disponibiliza.

11.3.10 Sistemas Homologados
O Grupo Lavoro possui sistemas homologados para todas as atividades previstas em seus processos. É proibido instalar sistemas que não tenham sido fornecidos pela empresa, mesmo que freeware, bem como o uso de software portátil (portable).
No caso de necessidade de uso de um sistema que não tenha sido homologado, os usuários devem solicitar o sistema ao seu gestor ou ao CAC. O sistema deve passar pela homologação antes de ser colocado em produção.
A homologação de novos produtos deve ocorrer em ambiente de rede controlado, que não concorra com o ambiente produtivo e avaliado pela equipe de segurança.

11.3.11 Cópias de Segurança

Os usuários devem manter todos os documentos eletrônicos importantes e de conteúdo corporativo nos servidores de arquivos, os quais possuem processos automáticos e periódicos de cópias de segurança. Todos os usuários têm o Onedrive que disponibiliza 1TB de dados. O Onedrive serve para armazenamento de dados utilizados pelo colaborador. Também está a disposição do colaborador o SharePoint, que é um repositório de dados para a empresa como um todo. Caso o colaborador queira disponibilizar/compartilhar os dados com outro colaborador, este dado deve ser compartilhado através do SharePoint.

11.3.12 Criptografia

Os usuários devem utilizar criptografia nas informações sempre que a mesma for classificada como secreta. A área de segurança da informação deve ser consultada para os devidos procedimentos.

11.3.13 Descarte e Reutilização de Equipamentos

Quando do descarte ou reutilização de um equipamento, seus discos rígidos e eventuais outras mídias devem ter seus dados totalmente sobrescritos de tal maneira que o acesso ao conteúdo seja impossibilitado, antes de serem reutilizados ou descartados. A equipe de segurança da informação e tecnologia da informação irão realizar tais procedimentos para manter o nível de segurança elevado.

11.3.14 Mídias Removíveis

Como mídias removíveis, para efeito desta Política de Segurança, se entende: modem 3G e 4G, disquete, CD-ROM, CD-R, CD-RW, DVD, DVD-R, DVD-RW, flashdrivers, pen drives, cartões de memória e similares.

11.3.14.1 Descarte de Mídias Removíveis

As mídias removíveis devem ser destruídas ou devidamente formatadas antes do descarte, de tal maneira que o acesso ao conteúdo seja impossibilitado. Entrar em contato com equipe de segurança da informação e TI para execução dos procedimentos necessários.

11.3.14.2 Controles de Uso

O uso de mídias removíveis está proibido. Exceções podem existir, mas estas serão auditadas e controladas. Em especial a gravação de CD/DVDs deve ser feita apenas pelas pessoas autorizadas conforme procedimento da empresa.

Os dispositivos SD Card, USB como pen drives ou outro tipo de armazenamento de dados devem ser autorizados pelo Gestor da pessoa e posterior análise e autorização da equipe de Segurança da Informação (IT Security). Caso liberado, o colaborador deverá assinar um termo de responsabilidade/confidencialidade. O uso destes dispositivos está sujeito à monitoração e auditoria por parte da equipe de Segurança da Informação (IT Security).

11.3.14.3 Uso de Mídia Removível Particular

Não é permitido o uso de mídias removíveis particulares no ambiente do Grupo Lavoro. O uso deve ser considerado um caso especial e necessita de autorização formal conforme os procedimentos da empresa.

11.3.15 Guarda do Equipamento

O usuário que utiliza sempre ou na maior parte do tempo o mesmo computador para executar suas tarefas é considerado como responsável pelo equipamento. Se o equipamento foi danificado, perdido ou roubado deve informar prontamente ao CSL. O usuário também é responsável pela informação armazenada no equipamento. A definição de responsabilidade será definida de acordo com a análise do ocorrido e aplicada em conjunto pelas áreas de Segurança, Recursos Humanos e Jurídico.

11.3.16 Comida e Bebida

Recomenda-se que os usuários evitem comer e beber enquanto utilizam os computadores. Normalmente estes equipamentos são sensíveis e podem sofrer danos em caso de um acidente.
Não é permitido comer e beber dentro de áreas como o Data Center e as salas de rack, que contêm equipamentos e sistemas críticos.

11.3.16.1 Fumo

É proibido fumar em áreas fechadas e principalmente em áreas com equipamentos e sistemas críticos.

11.3.17 Modems

Não é permitido o uso de modems nos computadores, salvo com autorização formal conforme procedimento da empresa. Usuários que precisem fazer conexões com computadores remotos devem solicitar ao CAC que providencie um acesso conforme os procedimentos do Grupo Lavoro.
Caso o computador possua um modem interno padrão, este deve ser removido ou desativado na instalação do sistema operacional.
No caso de uso de modem, o computador deve ser desconectado da rede interna do Grupo Lavoro.

11.3.18 Telefone

Para prevenir interceptação ou “grampo” os usuários devem evitar discutir informação sensível por telefone. Se a discussão de tal informação é imprescindível, os usuários têm que se abster de mencionar detalhes, tais como nomes de clientes, usuários, detalhes técnicos, projetos e outras informações sensíveis. Para estes casos recomenda-se a utilização de um sistema “misturador de voz” aprovado pela área de Segurança.
Em casos em que a discussão seja feita em lugares públicos, a atenção sobre as informações deve ser redobrada.

11.3.19 Ambientes de Rede

Responsabilidades do colaborador ou prestador de serviço nos acessos aos ambientes de rede:

1. Todos os assuntos inerentes a acessos aos ambientes rede do Grupo Lavoro, deverá ser solicitado através de chamado via Ticket de Suporte com a Área de Infraestrutura de TI.

2. Microsoft One Drive, Share Point e Outlook, são os ambientes homologado para guarda, utilização ou troca de arquivos em casos de uso individual ou compartilhado dentro das atividades inerentes ao trabalho realizado ao Grupo Lavoro .

11.3.20 Administrador Local

Mesmo aos usuários autorizados a ter perfil de administrador local, que necessitem efetuar alterações de endereço IP do computador ou efetuar alterações no registro de sistema que sejam extremamente necessárias para o funcionamento adequado de aplicações para as atividades de negócio do Grupo Lavoro, só serão aprovadas ou realizadas mediante abertura de chamado via Ticket de Suporte com a Área de Infraestrutura de TI.

Os usuários autorizados a ter perfil de administrador local, não estão autorizados a efetuar instalação de softwares nos equipamentos sob sua custódia, esta atividade deve ser solicitada via Ticket de Suporte com a Área de Infraestrutura de TI. O atendimento desta solicitação deverá ser avaliado e autorizado pela equipe de infraestrutura e em alguns casos para Área de Segurança da Informação (IT Security).
Em caso de uso indevido, o colaborador será notificado e o acesso será removido.

11.3.21 Cuidado com Informações Impressas

Informações não devem permanecer em equipamentos de fax e impressoras. Os usuários devem retirar os documentos imediatamente após a impressão.
Da mesma maneira documentos com informações sensíveis devem ser guardados adequadamente (cofres, gavetas malotes e armários com chave) conforme a criticidade das informações neles contidos.

11.3.22 Utilização de Máquinas Virtuais

É proibida a utilização ou manutenção de máquinas virtuais em equipamentos corporativos como desktops, notebooks e tablets sem a autorização da equipe de segurança da informação e suporte ao usuário. A autorização destas funcionalidades também está associada à disponibilidade de licenciamento de software.

11.4 POLÍTICA DE USO DE PORTÁTEIS E ACESSO REMOTO

11.4.1 Pré-requisito

Antes de ser concedido o acesso remoto ou o uso de um computador portátil, o usuário deve ter passado pela integração em segurança da informação e assinado eventuais termos de responsabilidade conforme os procedimentos da empresa.

11.4.2 Informando Perda ou Dano

Os usuários de equipamentos portáteis devem informar prontamente ao superior imediato qualquer dano ou perda de qualquer produto. Deve ser aberto um incidente de segurança para a perda ou roubo do equipamento. Para mais informações, consultar a Política de Gerência de Incidentes de Segurança.
Igualmente importante é informar imediatamente qualquer suspeita de quebra de segurança. A não informação da perda ou dano implicará na responsabilização do usuário.

11.4.3 Proteção de Informações

Todos os computadores portáteis com informações sensíveis são elegíveis para utilizar ferramentas de criptografia conforme os procedimentos da empresa. Adicionalmente, todo o acesso remoto a informações do Grupo Lavoro deve ser feito utilizando uma conexão criptografada.
Deve-se utilizar senha de acesso para a proteção de portáteis como smartphones e celulares que possuam informações sensíveis, seguindo as considerações descritas no item 11.2.9.

11.4.4 Uso Autorizado

O computador portátil disponibilizado pelo Grupo Lavoro deve ser usado exclusivamente pela pessoa autorizada. O uso do equipamento por terceiros, sejam eles sócios, familiares, amigos ou qualquer outro é expressamente proibido.

11.4.5 Cópia de Segurança

Os usuários de computadores portáteis são responsáveis pelas informações neles armazenadas. É de responsabilidade do usuário manter os dados considerados sensíveis salvos em ambientes homologados Microsoft One Drive ou Share Point corporativo para que as devidas cópias de segurança sejam realizadas.

É estritamente proibido utilizar outros tipos de repositórios locais ou em nuvem que não sejam os homologados e autorizados pelo Grupo Lavoro.

11.4.6 Elegibilidade dos Acessos Remotos para Colaboradores

Os acessos remotos externos para colaboradores são exclusivos para plantonistas ou outras pessoas cuja necessidade de acesso seja reconhecida e aprovada pelo seu gestor, que deverão ser reconhecidos e autorizados pela área de Recursos Humanos.

Não é permitido conceder a realização de acesso remoto para pessoas que estão de férias, compensação de banco de horas, afastamento por licença médica ou licença maternidade e os acessos remotos autorizados serão revogados quando do início das férias ou afastamentos.

Os acessos remotos concedidos que não sejam utilizados por 60 dias serão revogados, e uma nova solicitação deverá ser feita caso seja novamente necessário o acesso.

11.4.6.1 Requisitos de Acessos para Colaboradores

Os acessos remotos devem ser estritamente controlados.

Em nenhum momento os colaboradores devem repassar seu login, senha a outras pessoas. Se identificado uso indevido, o acesso será removido.

Quando o acesso remoto via VPN é realizado, todas as outras redes são automaticamente desabilitadas, ficando o acesso restrito somente à rede corporativa do Grupo Lavoro, conforme procedimento de acesso remoto (VPN).

Equipamentos com configurações não padronizadas devem ser aprovados pela equipe de segurança da informação do Grupo Lavoro (IT Security).

Todos os computadores que se conectarem à rede corporativa do Grupo Lavoro via acesso remoto, devem possuir software de antivírus atualizado.

O “TERMO DE COMPROMISSO DE UTILIZAÇÃO DE REDE PARTICULAR VIRTUAL – VPN”
deve ser preenchido na solicitação do acesso remoto.

11.4.7 Requisitos de Acessos para Organizações

Acessos remotos para outras empresas devem ser realizados via VPN (site-a-site).

O termo de confidencialidade (NDA) deve ser preenchido, assinado e entregue à área de contratos do Grupo Lavoro antes que o acesso seja liberado. Além disso, faz-se necessário a assinatura do termo de responsabilidade VPN site-a-site.

A configuração da VPN (site-a-site) será realizada pela equipe de TI da em conjunto com a equipe técnica da empresa que deseja realizar a conexão de acesso remoto. Os acessos remotos de empresas terceiras devem ser realizados estritamente para interesse do negócio do Grupo Lavoro, com parceiros ou fornecedores e mediante autorização da equipe de Segurança da Informação (IT Security).

Acessos remotos realizados a partir de ferramentas de acesso remoto ou qualquer outra ferramenta de colaboração estarão sujeitos aos mesmos controles e poderão ser liberados por no máximo 7 dias após a aprovação do chamado.

Todos os acessos realizados via VPN deverão ser solicitados via chamado, com prazo máximo de 90 dias, podendo ser renovado mediante abertura de um novo chamado.
Os chamados deverão ter explicitados os horários em que os acessos serão concedidos (dias da semana, horário de início, horário de término), bem como a especificação da necessidade e tarefas a serem realizadas para que o acesso seja justificado. Os acessos deverão ser liberados apenas para o segmento de rede especificado na abertura do chamado. Não deve, portanto, ser liberado o acesso a todo o segmento de rede.
Os acessos remotos de terceiros são autorizados em caráter de suporte, apenas para servidores que estão em ambiente de desenvolvimento/homologação. Caso seja necessário o acesso remoto de terceiros ao ambiente de produção este deverá ser acompanhado/monitorado por um responsável técnico do Grupo Lavoro, mediante a assinatura e aprovação do Diretor da área solicitante no "TERMO DE RESPONSABILIDADE – VPN SITE-A-SITE – AMBIENTE DE PRODUÇÃO", bem como aprovação da Diretoria de TI.
Toda e qualquer alteração feita no ambiente do Grupo Lavoro pela empresa terceira, será de responsabilidade do colaborador solicitante do acesso remoto.

11.4.8 Uso de Equipamentos Particulares

Não é permitido acesso à rede local e sem fio (wireless) corporativa do Grupo Lavoro por meio de equipamentos particulares como notebooks, tablets entre outros.
Aos colaboradores, havendo a necessidade de uso destes equipamentos, deve ser efetuada a solicitação de compra deles.
Aos prestadores de serviço com equipamentos particulares e que necessitem de acesso à rede sem fio, o acesso à rede "guest" ou a rede "partner" será liberado por prazo máximo de 30 dias.

11.4.9 Redes sem Fio

Os usuários não devem utilizar redes sem fio, como wi-fi ou modem via telefone celular (GPRS, 3G, 4G etc.), ao mesmo tempo em que o computador esteja conectado à rede corporativa do Grupo Lavoro, a menos que estes sejam formalmente aprovados e fornecidos pelo Grupo Lavoro.
O mero uso de protocolos de comunicações digitais em lugar de protocolos de comunicações analógicos tradicionais não qualifica o sistema como seguro.
As redes sem fio disponíveis são:

- Corporativo: para uso exclusivo de colaboradores do Grupo Lavoro que utilizam notebooks;
- Visitantes: para uso exclusivo de visitantes.

11.4.10 Exposição Pública

Material sensível não deve ser lido, manuseado ou discutido em: elevadores, restaurantes, aviões, ônibus, metrô, trens ou em outros lugares de acesso público.

11.4.11 Bagagem

Os equipamentos portáteis, como notebook, smartphone, laptop e outros computadores transportáveis que contenham informação sensível não podem ser despachados como bagagem. Para evitar danos e roubo, esses equipamentos têm que permanecer na posse do viajante como bagagem de mão.

11.4.12 Termo de Responsabilidade

Equipamentos portáteis e outros equipamentos de sistemas de informação, não devem deixar os escritórios do Grupo Lavoro sem que o portador assine um termo de responsabilidade.

11.4.13 Proteção Física de Equipamentos Portáteis

Os equipamentos portáteis quando não estiverem em uso devem sempre estar com o devido bloqueio de acesso das credenciais de usuário.

11.4.14 Gerenciamento de Dispositivos Móveis (MDM)

Os dispositivos móveis fornecidos pelo Grupo Lavoro (tais como celulares, tablets e notebooks) poderão conter ferramentas de controle e rastreabilidade. Não é autorizada a remoção e ou alteração das configurações sem o consentimento da área de segurança da informação. Estas ferramentas poderão sofrer atualizações, e neste caso serão previamente notificadas.

11.5 POLÍTICA DE ACESSO À INTERNET

11.5.1 Confiabilidade da Informação

Toda a informação vinda da Internet deve ser considerada suspeita até que se confirme o contrário. Não há nenhum processo do controle de qualidade na Internet, e uma quantidade considerável de informação é ultrapassada, imprecisa ou falsa. Em muitos casos, a informação falsa tem por objetivo fraudar o usuário.

Antes de usar uma informação recebida via Internet para finalidades de tomada de decisão, os usuários devem validar essa informação em pelo menos mais uma fonte confiável.

11.5.2 Verificação de Vírus

Todos os arquivos recebidos através da Internet devem ser verificados através das ferramentas adequadas fornecidas pelo Grupo Lavoro. Esta verificação visa evitar a infecção dos computadores por vírus ou outros programas maliciosos. O uso de assinatura digital ou criptografia não assegura a ausência de vírus.

11.5.3 Falsificação de Identidade

Antes que os usuários forneçam informações, contratem serviços ou efetuem qualquer outra transação, a identidade dos indivíduos e das organizações contatadas deve ser confirmada. A confirmação da identidade é executada idealmente através das assinaturas digitais ou dos certificados digitais, mas nos casos em que estas não estão disponíveis, outros meios tais como o contato pessoal, vídeo conferência e as conversações telefônicas podem ser usados.

11.5.4 Divulgação de Informações

Os usuários não devem divulgar informações internas através da Internet, por exemplo em mídias sociais ou blogs. Informações que de algum modo possam afetar o Grupo Lavoro nas suas relações com os clientes, fornecedores ou imagem pública são expressamente proibidas.

A divulgação de informações ao público deve ser efetuada através da área de Comunicação Corporativa.

11.5.5 Autenticação do Usuário

Todos os usuários que estabeleçam uma conexão com a Internet devem ser autenticados antes de ter o acesso permitido. Os registros da autenticação bem como informações complementares como: data e hora, volume de tráfego, endereços IP's, origem e destino da conexão devem ser armazenados e constantemente verificados. Estes registros ficarão armazenados por um prazo de 6 meses para registro de acesso a aplicações de internet, conforme o Marco Civil da Internet, lei 12.965/2014.

11.5.6 Senhas de Acesso

Os usuários não devem usar, em sites da Internet, as mesmas senhas que utilizam nos sistemas internos da empresa. Existem sites cujo único objetivo é capturar senhas de usuários dessa forma.

Sempre que possível os usuários não devem armazenar suas senhas, principalmente em softwares de navegação (browsers). Para os casos em que as senhas têm um nível de complexidade alto, softwares seguros de armazenamento de senhas poderão ser utilizados. A definição de quais os softwares seguros de armazenamento de senhas serão utilizados deverá ser definido pela equipe de Segurança da Informação (IT Security).

11.5.7 Uso Pessoal

Os usuários não devem utilizar-se da Internet ou outros sistemas de informação interna de maneira que a sua produtividade ou de outros usuários seja prejudicada.

A navegação ou acesso a locais com conteúdo abaixo relacionados é expressamente proibida, a menos que faça parte das suas atividades diárias de trabalho:

1. Vírus, jogos, pornografia;
2. Sons, vídeos, imagens não relacionadas com o trabalho;
3. Conteúdos sobre orientação sobre partidos políticos, religiosa, racial, sexual ou tratando de qualquer atividade ilegal.

11.5.8 Registros

O Grupo Lavoro se reserva o direito de registrar os sites visitados, os "downloads" efetuados, o tempo de acesso e a informação consultada.

A solicitação dos registros para eventuais análises deve ser efetuada à área de Segurança Empresarial.

11.5.9 Controle de Conteúdo na Internet

Com o intuito de diminuir os riscos de segurança à rede, o Grupo Lavoro dispõe de ferramentas de controle e otimização do uso da Internet.

Os usuários não devem burlar os controles das ferramentas de controle e otimização da Internet.

As ferramentas analisam o endereço (URL) dos sites visitados e efetua organização em categorias. As categorias podem possuir maior ou menor restrição de acesso, de acordo com as políticas do Grupo Lavoro.

Sua ação consiste em identificar o conteúdo do site a ser acessado e, de acordo com as políticas definidas pelo Grupo Lavoro para cada uma das categorias de conteúdo encontrados, nega, permite e controla o acesso para o usuário da rede.

As ferramentas atuam de maneira preventiva para impedir que programas maliciosos como vírus cavalos-de-troia entre outros, se instalem na rede do Grupo Lavoro e evitando que ocorra perda ou mau uso da banda de acesso à Internet.

As políticas de acesso à internet podem ser mais/menos permissivas desde que solicitado pelo gestor da área e o acesso não traga riscos para o ambiente do Grupo Lavoro. O gestor torna-se responsável pelas liberações solicitadas mediante chamado via Ticket na Área de Suporte de Infraestrutura de TI.

Em hipótese alguma o acesso à internet concedido aos colaboradores poderá ser IRRESTRITO. Algumas categorias de sites devem ser mantidas proibidas para garantir a integridade do ambiente.
Mesmo que possua NDA assinado, documentos não podem ser compartilhados na internet, para uso com terceiros.

11.5.10 Softwares de Mensagens Instantâneas

A troca de mensagens instantâneas por qualquer pessoa somente é permitida a partir de software homologado pelo Grupo Lavoro para este fim. A utilização de qualquer outro software de mensagem instantânea é proibida, salvo exceções para utilização em entrevistas ou para Suporte, com a devida autorização do Diretor da Área. Este acesso não é permitido para uso particular, caso seja identificado, o colaborador poderá ser notificado e o acesso será revogado.

11.5.11 Utilização de Serviços de Computação na Nuvem

A utilização de serviços de computação em nuvem para fins de trabalho, somente serão permitidos para ferramentas contratados e homologadas pelo Grupo Lavoro.
Não é permitida a utilização de contas pessoais em serviços na nuvem para armazenamento, manipulação ou troca de informações relacionadas com a empresa ou dados de propriedade do Grupo Lavoro.

11.5.12 Utilização de Mídias Sociais

Os usuários não devem utilizar as Mídias Sociais de forma que prejudique a imagem do Grupo Lavoro, prezando sempre a confidencialidade das informações. O Grupo Lavoro possui equipes responsáveis por responder aos usuários que entram em contato através das Mídias Sociais.
As seguintes práticas são proibidas:

1. Exposição de assuntos relativos à empresa;
2. Divulgação de dados confidenciais, resultados, informações sobre sistemas internos;
3. Publicação de fotos e vídeos com o logo do Grupo Lavoro;
4. Falar ou responder clientes em nome do Grupo Lavoro;
5. Utilização de linguagem inadequada em referência a clientes, concorrência ou do próprio Grupo Lavoro.

11.6 POLÍTICA DE USO DE CORREIO ELETRÔNICO

11.6.1 Propriedade da Companhia

Como uma ferramenta de produtividade, o Grupo Lavoro encoraja o uso do correio eletrônico.
O seu uso implica o reconhecimento de que os sistemas de comunicações eletrônicas e todas as mensagens geradas ou transmitidas através dos mencionados sistemas são de propriedade do Grupo Lavoro, podendo ser monitoradas ou auditadas a qualquer momento sem aviso prévio.

11.6.2 Uso Autorizado

Os sistemas de comunicações eletrônicas do Grupo Lavoro devem ser usados unicamente para atividades do trabalho. Para o uso do correio eletrônico é obrigatória a utilização de senha e Login pessoal e intransferível.
O uso pessoal ocasional é permissível desde que:

1. Não interfira com a produtividade;
2. Não tenha prioridade sobre nenhuma atividade do Grupo Lavoro;

3. Não seja proibido pela Política de Segurança, seus anexos e procedimentos.

11.6.3 Regras para Criação de Contas de E-mail

Na composição dos nomes de contas de email, deverá ser seguido um dos seguintes modelos de criação, para a conta de e-mail de terceiros há modelos específicos:

a. <nome>.<sobrenome>;
b. <nome>.<penúltimo sobrenome>;
c. <nome>+<primeira letra do segundo nome>.<sobrenome>;
d. <nome>.<sobrenome>+<dígitos (2, 3, 4,...) >.
e. <nome>.<sobrenome.terceiro>;
f. <nome>.<penúltimo sobrenome.terceiro>;
g. <nome>+<primeira letra do segundo nome>.<sobrenome>.terceiro;
h. <nome>.<sobrenome>+<dígitos (2, 3, 4,...).terceiro >.

11.6.4 Proibições

As seguintes atividades são estritamente proibidas, sem exceções:

1. Enviar mensagens não solicitadas, incluindo o envio de "junk mail" ou outros materiais de propaganda a indivíduos que não tenham requisitado especificamente estes materiais (e-mail spam);
2. Qualquer forma de assédio via e-mail, quer através da linguagem, frequência, tamanho ou conteúdo das mensagens;
3. Forjar o cabeçalho dos e-mails;
4. Postar e-mails ou mensagens não relacionadas ao negócio do Grupo Lavoro em listas ou newsgroups;
5. Utilizar o e-mail do Grupo Lavoro para fins não relativos ao negócio do Grupo Lavoro;
6. É proibida a utilização de correio eletrônico particulares, tais como Hotmail, Zipmail, Gmail, Yahoo ou qualquer outro para atividades do Grupo Lavoro.
7. Utilizar o correio eletrônico particular para transmitir informações pertinentes o Grupo Lavoro.

11.6.5 Armazenamento da Senha

Embora os clientes de correio eletrônico ofereçam essa opção, os usuários não devem armazenar sua senha de acesso para evitar acessos não autorizados.

11.6.6 Mensagens Genéricas

Com a exceção de emergências e manutenção de sistema, só devem ser usadas mensagens "para todos" pela área de Comunicação Interna.

11.6.7 Atualização dos Grupos de E-mails

Os responsáveis pelos Grupos de E-mails do seu departamento são os gerentes, onde devem atualizar periodicamente os grupos a equipe de TI, garantindo que todos os endereços receberão as comunicações enviadas, bem como solicitar a exclusão do grupo se este não estiver sendo utilizado.
Os gerentes de cada departamento, deverão indicar substitutos caso se desliguem da empresa ou mudem de área, mantendo assim a responsabilidade pelos grupos atualizada.

11.6.8 Identidade de Usuário

Falsear, obscurecer, suprimir ou substituir a identidade de um usuário em um sistema de comunicações eletrônicas é proibido. O nome do usuário, o endereço de correio eletrônico e afiliação organizacional devem, obrigatoriamente, corresponder à verdade.

11.6.9 Privacidade

O Grupo Lavoro vem adequando suas tecnologias para auxiliar na questão de privacidade com novas tecnologias, procedimentos, políticas e treinamentos. O Grupo Lavoro não pode garantir que as comunicações eletrônicas serão privadas. Os usuários devem estar atentos ao fato que comunicações eletrônicas podem, enquanto dependendo da tecnologia, ser interceptadas, impressas ou armazenadas por terceiros.

11.6.10 Proteção

Todos devem estar cientes que os sistemas de comunicações eletrônicas não são protegidos automaticamente.

O Grupo Lavoro vem trabalhando constantemente nas políticas, procedimentos, tecnologia de ponta e treinamentos para auxiliar a proteção dos dados de clientes, fornecedores e colaboradores.

Informações sensíveis devem ser protegidas com o uso de criptografia. Na impossibilidade de proteger a informação com criptografia via certificado digital, deve ser utilizado arquivo compactado com senha seguindo os requisitos mínimos de complexidade (caracteres especiais e alfanuméricos).

Todos devem ter extrema cautela ao abrir e-mails com anexos recebidos de fontes desconhecidas, pois eles podem conter vírus, códigos maliciosos, cavalos-de-troia ou outros tipos de ameaças digitais. Anexos e mensagens devem ser verificados com antivírus.

11.6.11 Mensagens Monitoradas

O conteúdo e o uso de sistemas de comunicações fornecidos pelo Grupo Lavoro poderão ser monitorados para apoiar as atividades de manutenção, segurança, auditoria e outras investigações. Os usuários devem utilizar as comunicações eletrônicas tendo ciência de que o Grupo Lavoro se reserva o direito de examinar o conteúdo das mesmas a qualquer momento.

A solicitação dos registros para eventuais análises deve ser efetuada à área de Segurança da Informação (IT Security).

11.6.12 Proteção Contra Mensagens Maliciosas e Vazamento de Informações

Com o intuito de diminuir os riscos de segurança à rede, o Grupo Lavoro dispõe de ferramentas de proteção contra mensagens maliciosas e vazamento de informações sigilosas da empresa. Os usuários não devem burlar os controles de tais ferramentas.

As ações das ferramentas consistem em identificar o conteúdo das mensagens e de acordo com as políticas definidas pelo Grupo Lavoro, controlar, negando ou permitindo o envio e recebimento das mensagens.

As ferramentas atuam de maneira preventiva para impedir que programas maliciosos como vírus cavalos-de-troia entre outros, se instalem na rede do Grupo Lavoro e evitando que ocorra vazamento de dados sigilosos da empresa.

11.6.13 Revelação Investigativa

Pode ser necessário que a equipe de TI/segurança da informação/incident handler revise o conteúdo das comunicações de um usuário individualmente durante o curso de resolução de problemas. A TI/segurança da informação/incident handler, no entanto, é proibida de revisar o conteúdo das comunicações de um usuário movido por curiosidade ou qualquer outro motivo pessoal.

11.6.14 Perfis Diferenciados das Contas de E-mail

As caixas de e-mail de colaboradores e prestadores de serviços do Grupo Lavoro possuem os mesmos perfis de cotas, 99GB de armazenamento, devido ao licenciamento padrão.

Todas as contas possuem limites de destinatários padrão, 10 mil / dia. Caso seja necessário aumento de capacidade, deverá ser aberto chamado via Ticket de Suporte com a Área de Infraestrutura de TI.

Para envio e recebimento de mensagens o tamanho padrão para todos os colaboradores e prestadores de serviço é de aproximadamente 20 MB.

Caso seja necessária a transmissão de arquivos maiores, a ferramenta para Transferência Segura de arquivos deve ser utilizada.

11.6.15 Conteúdos de Mensagens

Os usuários não devem utilizar termos obscenos ou observações pejorativas em mensagens de correio eletrônico/ferramentas de comunicação.

É proibido utilizar os recursos de correio eletrônico/ferramentas de comunicação para:

1. Arquivos contendo vírus, jogos, música, pornografia, vídeo ou imagens não relacionadas com o trabalho;
2. Mensagens de propaganda ou venda de produtos com fins particulares;
3. Cartas de corrente ou “spam”;
4. Mensagens de orientação política, religiosa, racial, sexual ou que configurem atividade ilegal.

11.6.16 Mensagem para Fora do Grupo Lavoro

Todo e-mail enviado por colaboradores ou prestadores de serviços do Grupo Lavoro para newsgroups devem conter uma mensagem explicando que as opiniões contidas nele são suas e não necessariamente do Grupo Lavoro, a menos que o e-mail tenha sido postado para atividades do negócio.

Os usuários de comunicações eletrônicas devem tomar toda precaução ao remeter mensagens.

Não devem ser remetidas informações sensíveis a pessoas fora do Grupo Lavoro sem a aprovação prévia do responsável pela informação. Todas as mensagens devem informar claramente que não expressam a opinião do Grupo Lavoro. A área de Tecnologia da Informação fica encarregada de configurar a assinatura padrão pré-definida em todos os computadores conforme abaixo:

Assinatura Padrão

Esta mensagem pode conter informações confidenciais ou privilegiadas. Se você recebeu esta mensagem por engano, você não deve usar, copiar, divulgar ou tomar qualquer atitude com base nestas informações. Solicitamos que você apague a mensagem imediatamente e avise o Grupo Lavoro enviando um e-mail para suporte@lavoroagro.com.

Opiniões, conclusões ou informações contidas nesta mensagem não necessariamente refletem a posição oficial da empresa.

Este e-mail não é um contrato, oferta ou aceitação de proposta. Só os representantes legais podem firmar compromissos em nome do Grupo Lavoro.

This message may contain privileged and confidential information for the use of the intended recipients only. If you are not an intended recipient then you should not disseminate, copy, or take any action based on its contents. If you have received this message in error then please notify LAVORO HOLDING GROUP by sending an e-mail message to suporte@lavoroagro.com immediately.
Views and opinions expressed in this message do not necessarily reflect the position of the company.
This email is not a contract, offer or acceptance of proposal. Only its legal representatives can bind LAVORO HOLDING GROUP.

11.6.17 Mensagens Suspeitas

Os Usuários devem abrir chamado para a área de Segurança da Informação (IT Security) das mensagens suspeitas que receberem, quando julgarem que isso é necessário para prevenir outros usuários. Em especial, mensagens com o objetivo de fraudar o usuário ou a empresa devem ser enviadas através da abertura do chamado "Solicitação de Análise e Bloqueio de SPAM", disponível no Portal CAC.

11.6.18 Armazenamento e Retenção de Mensagens

Não há um prazo máximo para que as mensagens de correio eletrônico sejam mantidas no sistema de correio eletrônico do Grupo Lavoro para posteriormente serem apagadas. Contudo, o armazenamento de mensagens do servidor dependerá do espaço disponível na caixa postal do colaborador, conforme apresentado na tabela do item 11.6.14.
É responsabilidade de cada usuário armazenar as mensagens ou arquivos anexos que sejam necessários por prazo maior do que o estipulado nesta política de forma segura e de acordo com o seu nível de classificação.
As mensagens que já não sejam mais necessárias devem ser apagadas pelos usuários.

11.6.19 Mensagens não devem ser contratos

O Grupo Lavoro deve ser representado perante terceiros unicamente por seus representantes legais: diretores e procuradores que devem respeitar seus respectivos níveis de alçadas.
Nenhum Colaborador está autorizado a fazer ofertas, aceitar propostas ou comprometer-se em nome do Grupo Lavoro por e-mail ou de qualquer outra forma.
Ofertas, aceitações e contratos devem ser formulados por documentos escritos firmados pelos representantes legais do Grupo Lavoro.

11.7 POLÍTICA DE SEGURANÇA EM RECURSOS HUMANOS

11.7.1 Segurança na Seleção de Pessoal

Durante os processos de recrutamento e seleção, devem ser colhidas informações sobre o histórico funcional dos candidatos, bem como contatos de referência. Devem ser verificadas, conforme os requisitos legais (ver Política de Conformidade), as informações fornecidas para garantir que são autênticas. Assim que o processo seletivo seja finalizado ou os currículos analisados sejam dispensados, os mesmos devem ser removidos/excluídos dos sistemas e ou e-mails.

11.7.2 Responsabilidades

11.7.2.1 Contratação de Empregados, Estagiários e Temporários

O processo de seleção, treinamento, transferência e desligamento de empregados, estagiários e temporários é de responsabilidade da área de Recursos Humanos juntamente com o Gestor da área onde a pessoa exerce suas atividades.

11.7.2.2 Contratação de Prestadores de Serviço

O processo de seleção, e demais alinhamentos necessários para a prestação de serviços de terceiros é de responsabilidade do gestor da área contratante.

Cada gestor é responsável pelas ações dos seus prestadores de serviço. Deve solicitar o login (para os casos desta necessidade) através da abertura de chamados no CSL, ou solicitar renovação no caso desta necessidade e obrigatoriamente cancelar este login em casos de término do contrato.

11.7.3 Segurança na Integração

Os novos colaboradores ou prestadores de serviços devem passar por um processo de integração que inclua um treinamento em segurança da informação. Esse treinamento tem por objetivo deixar clara a importância da segurança da informação para o negócio do Grupo Lavoro e estimular o cumprimento voluntário da política.

Na integração, os colaboradores ou prestadores de serviços devem ser claramente informados das funções de segurança em que estarão inseridos, bem como das responsabilidades a eles atribuídas.

Durante o primeiro acesso à Rede/Intranet, os colaboradores e prestadores de serviços deverão assinar eletronicamente o documento indicando que leram a Política de Segurança da Informação e se comprometem a segui-la.

11.7.4 Termos de Confidencialidade e Responsabilidade

Cada novo colaborador ou prestador de serviço deve assinar os termos apropriados antes de receber acesso a qualquer ativo de informação do Grupo Lavoro conforme os procedimentos da empresa.

11.7.5 Desligamento

Quando do desligamento de pessoal, a área de Recursos Humanos em conjunto com o gestor do colaborador deve analisar a necessidade de realizar uma entrevista de desligamento. Caso seja realizada, na entrevista devem ser relembradas as responsabilidades com relação ao sigilo das informações manipuladas quando trabalhando no Grupo Lavoro, destacando que os compromissos de confidencialidade permanecem em vigor, mesmo depois de encerrado o contrato de trabalho.

As devidas providências devem ser tomadas para que sejam revogados todos os acessos lógicos e físicos da pessoa que está sendo desligada bem como a devolução de todos os ativos físicos pertencentes ao Grupo Lavoro como notebooks, desktops, celular/smartphone, assim como mídia ou cópia de alguma informação da empresa que esteja sob a custódia da pessoa.

Caso o usuário tenha cadastrado “Duplo” ou “Múltiplo Fator de Autenticação” (2FA ou MFA) em qualquer aplicativo ou dispositivo, deverá auxiliar no procedimento para desabilitar ou fornecer qualquer chave de acesso, PIN ou outros que sejam necessários.

Adicionalmente, não é permitida a gravação ou impressão de dados utilizados pelo colaborador durante o exercício de suas funções, independente da mídia utilizada ou dos sistemas onde os dados estão armazenados no momento do seu desligamento. Estas informações, uma vez armazenadas nos sistemas da empresa, são consideradas de propriedade do Grupo Lavoro.

11.7.6 Conscientização Periódica

Os colaboradores ou prestadores de serviços devem participar de reforços periódicos de conscientização em segurança da informação conforme o agendamento feito pela empresa. O conteúdo deste treinamento deve permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação e respondam de acordo com as necessidades do negócio.

11.8 POLÍTICA DE SEGURANÇA FÍSICA E DO AMBIENTE

11.8.1 Perímetros de Segurança

Para evitar acesso não autorizado, dano ou interferência aos sistemas de informação considerados sensíveis, perímetros de segurança devem ser claramente definidos. Salas de Servidores, Equipamentos de Rede, Telefonia, Geradores e No-breaks, devem possuir as devidas proteções utilizadas em perímetros de segurança.

Barreiras físicas e sistemas de controle de acesso devem ser implementados para garantir o acesso apenas por pessoas autorizadas.

Um perímetro de segurança deve ter, no mínimo, as seguintes características:

1. Paredes, portas e teto com solidez adequada;
2. Um sistema de portaria, recepção e identificação eletrônica para controle e registro dos acessos;
3. Câmeras de segurança.

Todo acesso ao ambiente do Grupo Lavoro deve ser precedido de uma identificação na portaria. A portaria deve, obrigatoriamente, solicitar um documento de identificação oficial (Carteira de Identidade ou CNH e passaporte, no caso de estrangeiros), para garantir a identidade do visitante.

O acesso de prestadores de serviço aos ambientes de trabalho internos do Grupo Lavoro necessita de autorização prévia e do acompanhamento de um responsável.

Os colaboradores ou prestadores de serviços devem sempre questionar a presença de pessoas não conhecidas ou não identificadas nos ambientes de trabalho interno do Grupo Lavoro.

Todas as atividades dentro de um perímetro de segurança devem ser previamente autorizadas e monitoradas conforme o nível de criticidade do perímetro.

As portas de acesso a um perímetro de segurança devem sempre ser mantidas fechadas e todos os trabalhos de prestadores de serviços externo devem ser acompanhados.

Todas as atividades executadas por prestadores de serviço dentro do datacenter / sala de telefonia deve ser acompanhadas durante todo o tempo por um empregado do Grupo Lavoro. Deve ser registrado um chamado no CSL contendo o motivo do acesso ao datacenter e aguardada a aprovação para o acesso.

Locais que processam informações sensíveis (por exemplo DATACENTER) devem ter esta identidade dissimulada a fim de não permitir sua identificação.

11.8.2 Visitantes

Visitantes devem ser sempre acompanhados e a visita deve ser previamente agendada e autorizada.

11.8.3 Área de Carga e Recebimento

O recebimento de cargas ou equipamentos deve ser efetuado somente pelas pessoas autorizadas.

11.8.4 Equipamentos e Instalações

Os servidores ou outros equipamentos considerados críticos devem ser protegidos contra ameaças físicas como: roubo, fogo, poeira, água, temperatura e outras ameaças relevantes ou que tenham sido identificadas anteriormente em análise de risco.
As seguintes atividades não são permitidas em áreas com equipamentos críticos:

1. Guarda de Materiais inflamáveis.
2. Comer e beber
3. Fumar.

O local onde são armazenados os servidores ou outros equipamentos críticos deve possuir verificação e monitoramento constante de temperatura, umidade e detecção de incêndio.

11.8.5 Energia Elétrica

Servidores e equipamentos considerados críticos ou sensíveis devem ser protegidos contra a interrupção de energia elétrica.

11.8.6 Cabeamento

Os cabos de transmissão elétrica, dados e comunicações devem respeitar as normas técnicas vigentes bem como devem ser protegidos fisicamente. Alterações em cabeamentos somente deverão ser realizadas mediante requisição de mudança e aprovação da área responsável do Grupo Lavoro.

11.8.7 Manutenção

Os equipamentos e sistemas devem receber a manutenção preventiva e corretiva de acordo com as especificações do fabricante. Para realização de alterações ou correções, será necessário preencher o formulário para gerenciamento de mudanças no ambiente.
Sempre que for necessária a retirada de equipamentos das dependências do Grupo Lavoro para manutenção, informações sensíveis devem ser previamente apagadas de tal maneira que o conteúdo não possa ser lido ou recuperado. O prestador de serviço que realizará essa manutenção, deverá assinar o termo de confidencialidade e responsabilidade.

11.8.8 Transporte de Material para Fora da Empresa

Equipamentos, mídias, licenças de software, informações ou qualquer outro ativo de propriedade do Grupo Lavoro não podem ser retirados da empresa sem autorização prévia.

11.8.9 Revisão de Acessos

Todos os acessos que se enquadram nas categorias de porta de acesso principal, portas de salas de servidores e portas de acesso a no-break, devem possuir revisão anual de acesso.

11.8.10 Uso de Crachá

Toda e qualquer pessoa que adentrar as Unidades do Grupo Lavoro deverá estar portando obrigatoriamente o seu próprio crachá, em local visível, que liberará seu acesso às áreas preestabelecidas.

Em algumas unidades do Grupo Lavoro já está implantado o sistema Anti-Passback, que tem a função de monitorar as entradas e saídas, de maneira que o colaborador tem seu crachá liberado para sair somente se sua entrada tiver sido registrada e, do mesmo modo, no caso de uma nova entrada, a liberação do crachá ocorre apenas se a saída tiver sido armazenada no sistema.

11.8.11 Seguro

Quaisquer eventos que causem danos materiais ou morais a pessoas ou bens de propriedade do Grupo Lavoro ou de terceiros devem ser imediatamente informados para o departamento de Seguros a fim de que seja emitido um aviso de sinistro e tomadas as demais medidas necessárias para garantir a cobertura.

11.9 POLÍTICA DE OPERAÇÕES E GERÊNCIA DE SISTEMAS

11.9.1 Documentação dos Procedimentos

Todas as atividades de gerenciamento das operações e comunicações devem estar formalmente documentadas conforme os padrões de documentação do Grupo Lavoro.

11.9.2 Segurança na Documentação dos Recursos de TI

A documentação dos recursos de Tecnologia da Informação deve ser armazenada em local seguro e o acesso deve ser restrito apenas às pessoas que necessitem das informações.

11.9.3 Inventário dos Recursos

A TI é responsável por manter um inventário de softwares e hardwares de propriedade do Grupo Lavoro ou sob sua guarda, identificando os proprietários.

11.9.4 Registro de Atividades

Todas as atividades executadas devem ser registradas apropriadamente no sistema de registro de atividades e/ou chamados.

11.9.5 Controle de Mudanças

Todas as mudanças em ambiente computacional de produção devem ter o planejamento, a comunicação e os registros apropriados ao seu nível de criticidade.
Mudanças críticas agendadas devem seguir processo formal de controle de mudanças e serem aprovadas com antecedência.
Sempre que possível, uma mudança deve ser planejada por uma pessoa e revisada/aprovada por outra.

11.9.6 Segregação de Funções

É responsabilidade da TI implementar a segregação de tarefas. As tarefas operacionais e de controle do sistema devem ser executadas por diferentes usuários sempre que possível.

11.9.7 Equipamentos Fora do Grupo Lavoro

Equipamentos ou sistemas que, mesmo fisicamente fora do Grupo Lavoro, desempenhem funções ou armazenem informações de propriedade do Grupo Lavoro ou sob sua guarda estão sujeitos às regras definidas nesta Política de Segurança. Mais informações podem ser consultadas na Política de Segurança Física e do Ambiente.

11.9.8 Planejamento de Capacidade

Os equipamentos e sistemas do Grupo Lavoro ou sob responsabilidade do Grupo Lavoro devem ser continuamente monitorados sob o ponto de vista de planejamento de capacidade.
Os administradores dos equipamentos e sistemas devem usar os dados de monitoração para planejar a capacidade dos ativos sob sua administração.

11.9.9 Cópias de Segurança
É responsabilidade da TI implementar um processo para realização de cópias de segurança dos dados armazenados e processados, exclusivamente, nos servidores corporativos; equipamentos como desktops e notebook não fazem parte do escopo. O processo deve contemplar as ações necessárias para a que as informações sejam recuperadas, em casos de emergências, no menor tempo possível.

11.9.9.1 Controle de Mídias Corporativas
É responsabilidade da TI proteger adequadamente as mídias corporativas (CDs, DVDs, Disquetes, Fitas, Flash Memories, etc.) que contenham informações sigilosas. Quando não mais necessárias ao uso empresarial, as mídias devem ser destruídas fisicamente.

11.9.9.2 Mídias de Backup
É responsabilidade da TI definir e implementar controles de proteção para as mídias de backup contra acesso não autorizado ou alteração indevida. Deve ser claramente definido quem são as pessoas autorizadas a enviar, transportar e receber as mídias. O transporte deve ocorrer em um período apropriado ao objetivo de tempo de recuperação para o ativo crítico.

11.9.9.3 Periodicidade
É responsabilidade da TI em comum acordo com a área solicitante e com legislações aplicáveis definir a frequência de execução do backup, critérios de extensão, tempo de retenção e testes de recuperação para as cópias de segurança realizadas.

11.9.9.4 Necessidades Adicionais
Caso a necessidade do proprietário da informação não seja atendida pelo procedimento de backup oficial, este deverá solicitar à TI a adequação do backup para sua necessidade. Estas necessidades devem ser baseadas na classificação das informações (grau de sigilo), requisitos legais e de negócio do Grupo Lavoro.

11.9.9.5 Cuidados Adicionais
As cópias de segurança devem ser armazenadas em locais protegidos, conforme padrões de segurança física e ambiental que assegurem a integridade, disponibilidade e confidencialidade dos dados contidos nestas mídias.
Deve existir um controle centralizado e atualizado que contemple o inventário de todas as cópias de segurança realizadas no Grupo Lavoro.

Toda cópia de segurança de sistemas críticos deve ser realizada, no mínimo, em duas vias completas e recentes, armazenadas em locais distintos com os devidos controles de acesso e retiradas.
Incluir todos os dados e softwares necessários para dar suporte às atividades de negócios essenciais e aos planos de contingência.

Deve existir um processo de revisão periódica do procedimento de backup e processos de recuperação de cópias de segurança.
A restauração de uma cópia de segurança somente pode ser realizada através de uma autorização formal do proprietário ou depositário das informações contidas na mídia, devendo tal autorização ser arquivada para posterior auditoria.
Toda a recuperação e/ou restauração de uma cópia de segurança deve ser realizada em um ambiente diferente do original, sempre que tecnicamente possível, evitando danos aos dados atuais.
Toda cópia de segurança deve ser testada periodicamente, assegurando a integridade e a possível restauração dos dados.
As cópias de segurança de dados críticos e sensíveis do Grupo Lavoro devem possuir senhas de acesso e ou dispositivos de criptografia que impossibilite a restauração dos dados fora do ambiente do Grupo Lavoro.

11.9.9.6 Testes de Recuperação

A recuperação de sistemas, dispositivos, softwares e informações são realizadas pelas equipes que compõem a Diretoria de TI.
Os testes de recuperação deverão ser executados pelo menos uma vez a cada seis meses, focando recuperação parcial de um sistema. Entende-se por parcial: a recuperação do banco de dados ou de alguns dos aplicativos que compõem o sistema. Preferencialmente serão realizados testes com os sistemas "core" da empresa. A recuperação de outros sistemas e dispositivos também poderão ser testadas.
Todos os testes deverão seguir os procedimentos definidos pelas equipes. Os testes deverão conter uma documentação completa de sua realização e registros de sucesso ou falha, sendo esta documentação objeto de auditoria.
A documentação dos testes e seus registros serão auditados pela equipe de Segurança da Informação (IT Security).

11.9.10 Sincronização de Relógio

Todos os equipamentos e sistemas do Grupo Lavoro ou sob responsabilidade do Grupo Lavoro devem ter relógio sincronizado com uma fonte confiável de hora. O padrão recomendado para esta configuração é o padrão BRT.

11.9.11 Monitoração de Disponibilidade

Todos os equipamentos e sistemas do Grupo Lavoro ou sob responsabilidade do Grupo Lavoro devem ser monitorados continuamente para detecção de indisponibilidade e de situações fora da normalidade operacional.

11.9.12 Registros de Auditoria

Todos os sistemas do Grupo Lavoro que trabalham com informações confidenciais, financeiras ou fazem algum controle de acesso (autenticação e autorização) devem possuir trilhas de auditoria e as mesmas devem ser gravadas e guardadas por um período mínimo de 05 anos.
Os registros devem armazenar pelo menos as seguintes informações:

1. Identificação do usuário;
2. Data e hora dos eventos;
3. Detalhes dos eventos;

4. Identidade do terminal de origem e de destino do evento;
5. Abertura de sessão;
6. Tentativa de abertura de Seção Inválida;
7. Encerramento de Seção;
8. Falhas de Sistema.

11.9.12.1 Atividades a serem Registradas Devem ser registradas as seguintes atividades:

1. Criar, ler, atualizar ou apagar informações confidenciais incluindo autenticações e senhas;
2. Criar, atualizar ou apagar informações confidenciais;
3. Iniciar uma conexão de rede;
4. Aceitar uma conexão de rede;
5. Autenticação e autorização para atividades cobertas pelos itens 1 e 2 como entrada e saída nos sistemas (login/logout);
6. Permitir, modificar ou revogar acessos, incluindo adicionar novos usuários ou grupos, trocar níveis de privilégios, permissões de arquivos, regras de firewall e senhas administrativas;
7. Trocas de configuração em sistemas, serviços, e infraestrutura de rede e telefonia, incluindo atualizações e patches de softwares ou outras instalações de softwares.
8. Registro de início ou parada de aplicações em produção (start/stop/restart).
9. Falha de algum processo, especialmente se devido à exaustão de recursos (como CPU, memória, conexões de rede, banda de rede, espaço em disco, ou outros recursos), falhas de serviços de rede como DHCP, DNS ou outra falha de hardware.
10. Detecção de atividades suspeitas/maliciosas como sistemas de detecção de intrusão ou prevenção (IDS/IPS), antivírus, anti-spywares e anti-spam.

Registros adicionais podem ser necessários para a monitoração de recursos específicos.
Uma análise de risco deve ser efetuada para identificar as necessidades.
Os registros de auditoria devem ser protegidos contra acesso ou modificação não autorizados.

11.9.12.2 Monitoramento dos Registros de Auditoria

Os registros de auditoria devem ser monitorados regularmente com o objetivo de corrigir falhas, identificar oportunidades de acesso não autorizado e assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas.
Havendo a necessidade a análise dos registros será efetuada pelas áreas responsáveis.

11.9.13 Senhas Administrativas

As senhas utilizadas para administração dos sistemas de informação devem ser trocadas periodicamente, conforme a Política de Controle de Acesso e Autenticação. Os prazos de troca para cada tipo de senha administrativa devem estar documentados.

11.9.14 Contas de Serviço

Nos casos em que sistemas necessitem de contas de serviço para qualquer finalidade, é responsabilidade da TI implantar os seguintes controles:

1. Preferência na utilização de um grupo de serviço para iniciar as aplicações. Assim, não é necessária uma senha e realiza-se a prevenção de acesso a equipamentos;
2. As contas de serviço devem ser inventariadas, devendo constar no inventário, no mínimo:
    a. Nome da conta;
    b. Objetivo;

c. Responsável;
d. Vigência;
e. Data da última troca de senha.

3. O acesso às contas deve ser controlado e restrito aos profissionais da TI que dela fazem uso;
4. O acesso e conhecimento das senhas devem ser formalmente registrados e vinculados aos profissionais da TI que respondem pela administração do sistema;
5. No caso de sistemas críticos, deve ser avaliada a guarda compartilhada da senha;
6. Deve ser estabelecido um procedimento de substituição periódica ou sob demanda desta senha, como por exemplo, nos casos de desligamento do responsável pela conta de serviço;
7. A criação das contas de serviço deve ser autorizada pela equipe de Segurança da Informação (IT Security).

11.9.15 Contingência

É responsabilidade da TI implementar e testar um plano de contingência, sempre que um equipamento ou sistema seja uma parte crítica de um processo importante para o Grupo Lavoro. Mais informações podem ser consultadas na Política de Continuidade de Negócios.

11.9.16 Prestadores de serviços

O trabalho de prestadores de serviços na Sala de Servidores, Telefonia, no-breaks e Geradores deve ser previamente autorizado e acompanhado durante todo o tempo.
Caso tenham necessidade de acesso a informações sensíveis, os prestadores deverão assinar um termo de confidencialidade. Registrar um chamado prévio para autorização, explicando a necessidade e registrando o acesso. Mais informações podem ser consultadas através da Política de Segurança Física e do Ambiente.

11.9.17 Instalação Padrão e Mídias Originais

É responsabilidade da TI padronizar a instalação inicial dos sistemas. Deve-se evitar a personalização/customização de pacotes de software sempre que possível. Um conjunto padrão de instalação de software deve ser preparado e mantido em local seguro. Estas cópias padrão deve ser usadas para a recuperação de infecções por vírus de computador, falhas do disco rígido e outros problemas do equipamento.
É responsabilidade da TI implementar em todas as estações de trabalho um sistema de proteção contra programas maliciosos.

11.9.18 Gerenciamento e Controle de Estações

Toda estação de trabalho deve possuir software de gerenciamento e controle, para monitoramento de atividades e assistência ao usuário de forma remota.
O acesso à estação de trabalho do usuário, por meio do software de gerenciamento, deve ser autorizado por ele.

11.9.18.1 Instalação Padrão para Estação de Trabalho

Todo dispositivo de entrada e saída de dados, como Bluetooth, modem, leitor e gravador de CD/DVD, WiFi, portas USB, não se limitando a estes, deve ser desabilitado antes da liberação da estação de trabalho para o usuário. Este item não se aplica a teclados, mouses, monitores e placas de rede. Havendo a necessidade de uso o acesso deve ser formalmente solicitado e autorizado pelo gestor,

bem como analisado e autorizado pela equipe de Segurança da Informação (IT Security). Somente flashdrivers e pendrivers autorizados pela equipe de segurança e cadastrado via GPO devem ser liberados.
Toda estação de trabalho, quando tecnicamente viável, deve possuir lacre de segurança, controlado e inventariado pela TI.

11.9.19 Licenças de Software

As licenças de softwares adquiridos pelo Grupo Lavoro devem ser registradas e armazenadas em local seguro.
É vedado o uso de uma licença pessoal por duas ou mais pessoas, bem como o uso de qualquer software sem a devida licença ou de forma contrária à autorizada pelo licenciante.

11.9.20 Dos Endereços de Rede (IP)

O endereçamento IP das estações de trabalho dos equipamentos conectados à rede é dinâmico e atribuído automaticamente. A utilização de endereços fixos deve ser solicitada pelo usuário à equipe de TI.

A TI deve implementar controles para restringir ou detectar equipamentos não autorizados na rede do Grupo Lavoro.
Os servidores e impressoras devem possuir endereçamento fixo, fornecido pela equipe de TI. As alterações devem ser previamente notificadas.

11.9.20.1 Segregação de Redes

A TI é responsável por implementar controles para segregar as redes de dados em domínios lógicos com a finalidade de diminuir a oportunidade de acesso não autorizado. O tráfego entre as redes deve ser analisado para garantir que a Política de Segurança da Informação está sendo cumprida.
As autorizações de acessos entre redes devem ocorrer mediante chamado.

11.9.21 Gerenciamento das Redes

As redes de dados devem ser monitoradas para detectar ameaças e garantir segurança e níveis de serviço estabelecidos.

11.9.22 Acesso Remoto

É responsabilidade da TI garantir que todo acesso remoto aos sistemas do Grupo Lavoro seja feito através de VPN. Mais informações podem ser consultadas na Política de Uso de Portáteis e Acesso Remoto.

11.9.22.1 VPN

Toda solicitação de acesso VPN deve ser previamente autorizada pelo gestor e pela área de Recursos Humanos, após as aprovações será encaminhado à equipe de Segurança da Informação (IT Security) para análise e devido tratamento.
Todo equipamento que necessite acessar a rede do Grupo Lavoro remotamente deve possuir cliente VPN.
As configurações do cliente VPN devem obedecer aos critérios de segurança estabelecidos pela TI.

11.9.22.2 Perfil de Acesso

É responsabilidade da TI implementar controles que evitem a visibilidade, por parte de usuários com acesso remoto, de todo o ambiente de rede ou sistemas do Grupo Lavoro.
Nos casos em que a necessidade de negócio exija um acesso com esta visibilidade é responsabilidade da TI implementar controles para monitoração de cada acesso permitido.

11.9.23 Transferências de Informações

A troca de informações com terceiros em relação ao envio ou recebimento de arquivos, ordens de compra, recebimento ou outra forma de transferência de informações como B2B ou B2C, devem ser previamente autorizados pelo Responsável pela Informação. É responsabilidade da TI verificar as implicações e definir padrões de segurança adequados.
No mínimo, devem ser verificados e definidos:

1. Responsabilidades em caso de erro, alteração ou perda das informações;
2. Padrões técnicos e ferramentas utilizadas;
3. Procedimentos de proteção, verificação de envio, recebimento e rastreamento das mensagens;
4. Acordos de confidencialidade, responsabilidade e demais pertinentes.

11.9.24 Vulnerabilidades Técnicas

É de responsabilidade da TI obter em tempo hábil correções para vulnerabilidades em equipamentos e sistemas conforme são disponibilizadas pelos fabricantes.
Antes de serem colocadas em produção devem-se efetuar os devidos testes em ambiente segregado para não comprometer as operações (ver Controle de Mudanças) e questionar a equipe de segurança da informação se estão de acordo.

11.9.25 Isolamento de Sistemas Críticos

Sistemas considerados críticos devem ter ambiente computacional dedicado ou outros controles que garantam:

1. Somente acesso autorizado;
2. Integridade das informações;
3. Disponibilidade do sistema;
4. Plano de recuperação a desastre.

11.9.26 Proteção de Sistemas Disponíveis ao Público

Sistemas disponíveis ao público incluindo, mas não se limitando. Os sites do Grupo Lavoro, devem possuir controles para proteger as informações contra modificações não autorizadas.
Informações sensíveis que trafeguem em sistemas disponíveis ao público devem possuir controles que garantam a confidencialidade, integridade e disponibilidade dos dados. O acesso aos sistemas disponíveis ao público deve utilizar protocolos que garantam a confidencialidade dos dados trafegados como HTTPS.

11.9.27 Troca de Informações entre Sistemas

A troca de informações entre sistemas críticos deve possuir controles que garantam a proteção de dados sensíveis bem como a disponibilidade e integridade das informações. É responsabilidade da TI implementar os devidos controles para atingir este objetivo.

11.9.28 Aceitação de Sistemas

Novos sistemas e equipamentos bem como a alteração dos existentes devem possuir as devidas autorizações e testes antes da implantação em produção. Devem ser previamente acordadas as necessidades de acesso e a arquitetura de sistema.

11.9.29 Serviços Terceirizados

Os serviços de terceiros devem ser documentados e verificados sob o ponto de vista de segurança.
As alterações nos serviços prestados devem ser acompanhadas levando em conta a criticidade e os riscos ao Grupo Lavoro .
É responsabilidade da TI efetuar a avaliação dos serviços prestados por terceiros envolvendo os sistemas e equipamentos que estão sob sua custódia.

11.9.30 Uso de Chaves Criptográficas

Os usuários e sistemas devem utilizar para a proteção de informações sensíveis somente chaves criptográficas estabelecidas e autorizadas pelo Grupo Lavoro.
A emissão das chaves criptográficas cabe à TI, que deve estabelecer um processo de concessão, guarda e revogação das chaves.

11.9.31 Uso de Códigos Móveis

A TI deve implementar controles para que somente código móvel autorizado seja executado nos computadores que deles necessitem.

11.9.32 Segregação de Ambiente

Os ambientes de desenvolvimento, testes e produção devem ser ambientes totalmente distintos. Não é permitido efetuar desenvolvimentos e testes de sistemas em equipamentos de uso pessoal ou estações de trabalho conectadas à rede corporativa.

11.10 POLÍTICA DE AQUISIÇÃO, DESENVOLVIMENTO E IMPLANTAÇÃO DE SISTEMAS

11.10.1 Papéis e responsabilidades

11.10.1.1 Líder Técnico

O líder técnico tem a responsabilidade de interagir com a TI e/ou agentes de serviços externos, para certificar-se de que todas as definições de segurança tenham sido implantadas quando da aquisição, desenvolvimento ou manutenção de sistemas. Quando necessário, a TI pode consultar empresas especializadas em Segurança da Informação para avaliar se controles implantados estão de acordo com as boas práticas de Segurança da Informação.

11.10.1.2 Líder de Projeto

O líder de projeto executa a análise crítica das mudanças de software, considerando requisitos de qualidade e Segurança da Informação, o líder de projeto deve interagir com a TI em relação aos requisitos de Segurança da Informação.

11.10.2 Produtos de Terceiros

No caso de sistemas adquiridos externamente já completos, é responsabilidade do líder técnico seguir o processo de homologação de software que deve contemplar os requisitos de Segurança da Informação cabíveis. Os registros e documentos fiscais relacionados ficam sob responsabilidade da TI.

11.10.2.1 Envio de Dados para Terceiros

Havendo a necessidade no envio de dados confidenciais para fábricas de teste e fábricas de software para o desenvolvimento ou manutenção de sistemas existentes, devem ser empregados controles adequados para proteger as informações enviadas.

Os seguintes controles devem ser utilizados antes do envio dos dados:

1. Criptografia dos Dados Enviados;
2. Proteção Física das Mídias com os Dados;
3. Acordo de Confidencialidade assinado pela Empresa Terceira (NDA);
4. Embaralhamento de dados, quando possível.

É proibido prover informações sobre clientes, colaboradores ou outros prestadores de serviço do Grupo Lavoro para terceiros.

Outros controles devem ser aplicados conforme a sensibilidade dos dados e o meio de envio.

11.10.3 Padrões de Nomenclatura

Os sistemas devem ser desenvolvidos adotando uma nomenclatura padronizada, seja de tabelas, campos ou outros componentes necessários.

11.10.4 Validação de Dados

É responsabilidade do líder técnico do projeto definir controles de verificação de entrada e saída. O líder técnico do projeto deve indicar qual parte do processamento lidará com informações sensíveis. Para estes casos, a equipe de Segurança da Informação (IT Security) deve avaliar a necessidade de controles adicionais.

11.10.4.1 Dados de Entrada

Devem ser definidos padrões de verificação de consistência para os dados de entrada.

Normalmente os controles de consistência tratam de, entre outros:

1. Verificação de faixa de valores;
2. Verificação de caracteres inseridos;
3. Verificação de falta de dados ou valores incompletos;
4. Alterações indevidas, no caso de formulário em papel;
5. Identificação de responsabilidades e autorização para entrada de dados.

11.10.4.2 Processamento Interno

A metodologia de desenvolvimento deve possibilitar a identificação de partes do sistema que sejam considerados pontos críticos em termos de integridade, disponibilidade, confidencialidade, autenticidade, não repúdio e desempenho.

11.10.4.3 Dados de Saída

Devem ser implementados controles de verificação para identificar erros de processamento; recomenda-se a implantação de controles para, entre outros:

1. Verificação de erros de processamento, teste de validação;
2. Criação de telas e mensagens de erro genéricas;
3. Verificação e reconciliação caso necessário;
4. Atribuição de responsabilidades de acordo com verificação periódica dos dados de saída.

11.10.5 Trilhas de Auditoria

Operações críticas realizadas pelos sistemas devem conter mecanismos para rastreamento das ações realizadas, de acordo com as definições da Política de Operações e Gerência de Sistemas.

11.10.6 Autenticação e Segurança dos Dados

11.10.6.1 Controle de Acesso

É responsabilidade do líder técnico do projeto certificar-se que o novo sistema possua, no mínimo, as seguintes funcionalidades:

1. Possibilidade de integração com os mecanismos de autenticação em uso no Grupo Lavoro;
2. Possibilidade de troca de senha por parte do usuário;
3. Segurança no armazenamento de informações sensíveis de acordo com os padrões de segurança e criptografia definidos pelo Grupo Lavoro;
4. Possibilidade de implementação dos controles definidos na Política de Controle de Acesso e autenticação.

11.10.6.2 Autenticação e Integridade

É responsabilidade do líder técnico do projeto incluir controles de proteção e verificação aprovados pela TI, sempre que a especificação do sistema incluir a troca de dados ou mensagens sigilosas com outro sistema.

11.10.7 Verificação de Requisitos

É responsabilidade do líder técnico do projeto definir um plano de teste e homologação. Somente após conclusão, com êxito, das fases de teste e homologação o sistema poderá ser colocado em produção.

11.10.8 Segregação de Ambientes

Os ambientes de desenvolvimento, testes e produção, devem ser ambientes totalmente distintos. Não é permitido efetuar desenvolvimentos e testes de sistemas em equipamentos de uso pessoal ou estações de trabalho conectadas à rede corporativa.

11.10.9 Segregação de Funções

As tarefas de desenvolvimento, teste e passagem de sistemas para produção devem ser executadas por equipes diferentes ou, no mínimo, por usuários diferentes.

11.10.10 Dados para Teste de Sistemas

Durante o desenvolvimento e teste dos sistemas não podem ser utilizados dados reais dos sistemas em produção, sem a autorização do responsável pelo Ativo. Na necessidade de utilizar dados de produção as informações consideradas sensíveis devem ser descaracterizadas/anonimizadas.

11.10.11 Controle de Acesso às Fontes e Base de Dados

É responsabilidade do líder técnico do projeto definir mecanismos de proteção das bibliotecas de programas contra alterações não autorizadas. Em se tratando de bases de dados de produção, o acesso deve ser restrito ao menor número possível de profissionais e verificado periodicamente pelo líder

técnico do projeto. Caso seja comprovada a necessidade do acesso por outros profissionais, este deve ser liberado por um período determinado, necessário à execução da tarefa, e retirado em seguida. Durante o uso, o acesso deve ser monitorado pelo líder técnico do projeto.

11.10.12 Controle de Alteração de Software

Para toda alteração de software deve ser definido um procedimento de requisição e aprovação formal pelos responsáveis. Os controles e procedimentos devem conter no mínimo:

1. Registro da requisição de alteração;
2. Registro da versão em uso e da versão alterada;
3. Plano de instalação que leve em conta o tempo de paradas e possíveis perdas de produtividade;
4. Plano de reversão que leve em conta o tempo de paradas e possíveis perdas de produtividade;
5. Registro dos testes, apresentação dos resultados e aprovação da alteração pelos responsáveis.

11.10.13 Controle de Versão

A metodologia de desenvolvimento deve prever mecanismos para controle de versão de todos os softwares desenvolvidos ou customizados no Grupo Lavoro.

11.10.14 Controle Contra Ameaças Internas

A metodologia de desenvolvimento deve prever controles que ofereçam proteção contra ameaças tipo "bomba relógio", "cavalo-de-troia" ou similares. Deve ser considerada, no mínimo, a adoção dos seguintes controles:

1. Auditoria, mesmo que por amostragem, das fontes dos sistemas;
2. Verificação dos registros (logs) dos sistemas à procura de atividades incomuns;
3. Rígido controle de mudança quando o sistema operacional puder ser alterado.

Os sistemas desenvolvidos/adquiridos deverão ser instalados e processados em servidores do Grupo Lavoro.

11.11. POLÍTICA DE GERÊNCIA DE INCIDENTES DE SEGURANÇA

11.11.1 Comunicação de Incidente de Segurança

Violações à Política de Segurança da Informação constituem incidentes de segurança e devem ser comunicados. É responsabilidade de todos comunicarem incidentes assim que tomarem conhecimento da sua ocorrência ou da possibilidade de uma ocorrência.

11.11.1.1 Transgressões à Política de Segurança

Transgressões à Política de Segurança da Informação devem ser encaminhadas para a área de Segurança da Informação através do e-mail security@lavoroagro.com para que a situação seja avaliada e as devidas providências sejam tomadas.

11.11.1.2 Indisponibilidade de Sistemas

Em caso de indisponibilidade de sistemas a operação de TI, a área de Suporte a Infraestrutura deverá ser informada imediatamente através de ligação para o número (41) 3046 8643.

A partir desta comunicação as equipes responsáveis serão acionadas para análise e solução da indisponibilidade.

11.11.2 Tratamento e Melhoria Contínua

Após a comunicação, os incidentes devem ser tratados, evidências devem ser coletadas e um relatório final deve ser elaborado.

Comunicações consideradas como falsos positivos, ou seja, que não constituem incidentes, podem ser descartadas.

Os relatórios dos incidentes devem servir como entrada para o processo de melhoria contínua da segurança da informação e suas ações corretivas devem priorizar o tratamento sistêmico da segurança na empresa em vez de apenas correções pontuais.

11.11.3 Processo Disciplinar

É importante que as violações da Política de Segurança tenham um processo disciplinar adequado.

Pessoas que violem a Política de Segurança podem incorrer nas sanções previstas nesta política (ver Descumprimento das Normas – Capítulo 12).

11.11.4 Coleta de Evidências

A aplicação de sanções somente pode ser feita quando houver evidência inequívoca da responsabilidade.

Cabe exclusivamente à área de Ouvidoria/Canal de Denúncia conduzir as devidas investigações em caso de violações da Política de Segurança da Informação. Havendo a necessidade, outras áreas como o Departamento Jurídico, Recursos Humanos e a equipe de Segurança da Informação (IT Security), poderão prestar suporte para a equipe de Ouvidoria/Canal de Denúncia nas devidas investigações.

11.11.5 Contato com Autoridades e Grupos Especiais

A TI deve manter contato com Autoridades e Grupos de Segurança da Informação para o rápido atendimento em caso de incidentes de segurança da informação bem como atualização sobre as melhores práticas utilizadas no mercado.

11.12 POLÍTICA DE CONFORMIDADE

11.12.1 Identificação de Requisitos de Conformidade

Devem ser identificados, documentados e mantidos atualizados os requisitos de conformidade legal ou regulatórios para todos os ativos de informação do Grupo Lavoro. Esta identificação deve fazer parte do processo de análise e tratamento de riscos de segurança da informação.

Em nenhuma circunstância um colaborador ou prestador de serviço do Grupo Lavoro está autorizado a praticar atos que contrariem as leis aplicáveis, quando se utilizar de recursos pertencentes ao Grupo Lavoro.

Como referência, seguem algumas regras pertinentes – mas não se limitando a estas – que se aplicam as atividades do Grupo Lavoro:

Legislação: Pontos de Atenção e Disposições das Legislações Identificadas
Constituição Federal - Ponto de Atenção: Direito ao sigilo de dados
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas

hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Lei 8.078/90
Código de Defesa do Consumidor - Ponto de Atenção: Acesso do consumidor à suas informações em banco de dados de terceiros
Artigo 43: O consumidor [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. [...]

> § 2°A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

Lei Nº 9.610, De 19 de Fevereiro de 1998
Ponto de Atenção: Prevenção a Pirataria Lei de Proteção ao Direito Autoral
Art. 102. O titular cuja obra seja fraudulentamente reproduzida, divulgada ou de qualquer forma utilizada, poderá requerer a apreensão dos exemplares reproduzidos ou a suspensão da divulgação, sem prejuízo da indenização cabível.
Art. 103. Quem editar obra literária, artística ou científica, sem autorização do titular, perderá para este os exemplares que se apreenderem e pagar-lhe-á o preço dos que tiver vendido.
Parágrafo único. Não se conhecendo o número de exemplares que constituem a edição fraudulenta, pagará o transgressor o valor de três mil exemplares, além dos apreendidos.
Art. 104. Quem vender, expuser a venda, ocultar, adquirir, distribuir, tiver em depósito ou utilizar obra ou fonograma reproduzidos com fraude, com a finalidade de vender, obter ganho, vantagem, proveito, lucro direto ou indireto, para si ou para outrem, será solidariamente responsável com o contrafator, nos termos dos artigos precedentes, respondendo como contrafatores o importador e o distribuidor em caso de reprodução no exterior.

Decreto-Lei Nº 5.452, de 1 de maio de 1943
Ponto de Atenção: Revelação de Informações Sigilosas da Empresa Consolidação das Leis Trabalhistas (CLT):
Artigo 482, da CLT, que trata dos motivos autorizadores da demissão por justa causa, traz de forma expressa e destacada a hipótese de violação de segredo da empresa.

Código Penal -Ponto de Atenção: **Crime de revelação de informação sigilosa**
Artigo 154. Revelar a alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem. Pena - detenção, de três meses a um ano, ou multa.

Decreto Nº 6.523, de 31 de julho de 2008
Ponto de Atenção: Tempo de Atendimento ao Consumidor (indisponibilidade de sistemas que dão suporte ao SAC) e Sigilo dos Dados de Clientes
Art. 3o

> § 4o Regulamentação específica tratará do tempo máximo necessário para o contato direto com o atendente, quando essa opção for selecionada.

Art. 5o O SAC estará disponível, ininterruptamente, durante vinte e quatro horas por dia e sete dias por semana, ressalvado o disposto em normas específicas.
Art. 10. Ressalvados os casos de reclamação e de cancelamento de serviços, o SAC garantirá a transferência imediata ao setor competente para atendimento definitivo da demanda, caso o primeiro atendente não tenha essa atribuição.

> § 1o A transferência dessa ligação será efetivada em até sessenta segundos
> § 3o O sistema informatizado garantirá ao atendente o acesso ao histórico de demandas do consumidor.

Art. 11. Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento.

Art. 13. O sistema informatizado deve ser programado tecnicamente de modo a garantir a agilidade, a segurança das informações e o respeito ao consumidor.

Lei Nº 9.051, de 18 de maio de 1995
Ponto de Atenção: Solicitar certidões de antecedentes para contratação
Dispõe sobre a expedição de certidões para a defesa de direitos e esclarecimentos de situações
Lei 9.029, de 13.04.95
Ponto de Atenção: Solicitar certidões de antecedentes para contratação
(...) definiu ato discriminatório em seu artigo 1o da seguinte forma: "qualquer prática discriminatória e limitativa para efeito de acesso a relação de emprego, ou sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar ou idade, ressalvadas, neste caso, as hipóteses de proteção ao menor previstas no inciso XXXIII do art. 7º da Constituição Federal".

Lei 12.527, de 18.11.2011
Lei de acesso à informação
Garantir o direito fundamental de acesso à informação

Lei 12.737, de 30.11.2012
Código penal, fica acrescido dos seguintes arts. 154-A e 154-B.

Lei 12.965, de 23.04.2014
Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Lei 13.709, de 14.08.2018 (LGPD)
Ponto de Atenção: Tratamento de dados pessoais, inclusive nos meios digitais
Aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

11.12.2 Utilização do nome do Grupo Lavoro sem autorização

Os colaboradores ou prestadores de serviço são proibidos de realizarem ofertas de itens ou serviços a terceiros em nome do Grupo Lavoro sem a autorização desta ou utilizar o nome do Grupo Lavoro para benefício próprio.

11.12.3 Propriedade Intelectual

É proibida a violação de direitos de qualquer pessoa ou companhia protegida por direitos autorais, segredos de negócio, patentes ou propriedades intelectuais, leis ou regulamentações similares.
A mídia original deve ser mantida em local seguro e não deve ser usada para atividades diárias, mas reservada para recuperação de infecções de vírus, falhas do disco rígido e outras falhas.
As licenças de software adquirido pelo Grupo Lavoro devem ser registradas em sistema apropriado e armazenadas em local seguro.
As licenças de uso devem ser auditadas regularmente para garantir que somente softwares autorizados e devidamente licenciados sejam utilizados e identificar o número máximo de usuários licenciados.

Sendo assim, é proibida a cópia não autorizada de produtos protegidos por direitos autorais como digitalização e distribuição de fotografias de revistas, livros ou outras fontes, músicas, vídeos e softwares.

11.12.3.1 Conteúdo Desenvolvido no Grupo Lavoro

Todo conteúdo desenvolvido no Grupo Lavoro ou por ordem desta é considerado como propriedade intelectual da empresa, e a divulgação sem a devida autorização é proibida.

11.12.4 Proteção dos Registros Organizacionais

Os registros críticos da empresa devem ser protegidos contra perda, destruição e falsificação de acordo com os requisitos do negócio. Para isto, todos os registros devem ser protegidos fisicamente, com acesso controlado e identificado o seu tempo mínimo de retenção de acordo com a legislação e regulamentação vigentes.

Para evitar a deterioração dos registros deverão ser consideradas outras formas de armazenamento desde que garantida a autenticidade deles.

A recuperação dos registros deverá ser realizada em tempo aceitável, levando em consideração eventuais processos de auditoria ou legislação vigente.

11.12.5 Privacidade das Informações Pessoais

O Escritório de Privacidade de Dados do Grupo Lavoro é responsável por todos os processos definidos e implementados para controles, proteção das informações pessoais de clientes, colaboradores e prestadores de serviços.

O setor observa as legislações e/ou regulamentações vigentes para a realização da coleta, armazenamento, transmissão e descarte das informações pessoais.

Todos os assuntos inerentes ao tema “Privacidade de Dados”, devem ser encaminhados ao Escritório de Privacidade de Dados do Grupo Lavoro, aos cuidados do Encarregado de Dados Pessoais (DPO), através do e-mail: dpo@lavoroagro.com , que irá realizar o devido entendimento, encaminhamento ou tratamento da demanda.

11.12.6 Verificação da Conformidade Técnica

Os sistemas de informação devem ser verificados anualmente quanto à conformidade com os requisitos técnicos implementados. Tais verificações devem incluir testes de intrusão e verificações de vulnerabilidades técnicas realizadas por profissionais experientes e competentes para a sua execução. Esta verificação deverá ser executada por especialistas independentes contratados especificamente para esta finalidade. Esta verificação deverá servir de entrada para o processo de análise/avaliação de riscos da segurança da informação.

11.12.7 Processo de Auditoria

Deverá ser definido e implantado um processo de auditoria periódica de segurança da informação. A definição dos controles deverá ser realizada de acordo com a análise/avaliação dos riscos, regulamentações vigentes e dos requisitos de negócio.

A realização do processo de auditoria deverá ocorrer com periodicidade anual por auditores experientes e competentes para sua execução.

A verificação bem como a utilização das ferramentas deve ser controlada e efetuada somente por com autorização da equipe de Segurança da Informação (IT Security).

11.13 POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

Um processo de gestão de continuidade do negócio deve ser implementado para minimizar o impacto sobre a organização resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais, a um nível aceitável.

12 DESCUMPRIMENTO DAS NORMAS

É responsabilidade de todo colaborador ou prestador de serviço, zelar pelo cumprimento da Política de Segurança da Informação do Grupo Lavoro. Nos casos de descumprimento desta Política, o colaborador ou prestador de serviço que tomar conhecimento do fato deve relatar à Ouvidoria/Canal de Denúncia do Grupo Lavoro, por meio de telefone ou Portal de Internet disponibilizados. Em casos de incidentes de segurança a área de TI, se necessário, poderá notificar os colaboradores ou prestadores de serviço quanto ao descumprimento das normas de segurança da informação.

12.1 CANAIS

- https://www.canalconfidencial.com.br/lavoro/
- http://lavoroagro.com/canal-de-transparencia/
- security@lavoroagro.com e dpo@lavoroagro.com

12.2 PENALIDADES

Qualquer colaborador ou prestador de serviço que violar esta política está sujeito às sanções aplicáveis por lei ou contrato e normativos internos do Programa de Integridade do Grupo Lavoro, inclusive a demissão por justa causa no caso de empregado e a resolução por inadimplemento no caso do prestador de serviços.

13 APROVAÇÃO

VERSÃO	DATA	REVISÃO	RESPONSÁVEL
1.4	01/06/2021	Ajustes, revisão e envio para aprovação	Fernando Cesar de Oliveira
1.3	26/05/2021	Ajustes, revisão e envio para aprovação	Fernando Cesar de Oliveira
1.2	26/04/2021	Ajustes	Thiago Mendes da Silva
1.1	16/09/2020	Revisão e alteração	Thiago Mendes da Silva
1.0	02/09/2020	Emissão Inicial	Hubert Thomaz