PL-001

Política de Segurança da Informação

ÍNDICE

1 Introdução

A Política de Segurança da Informação (PSI), é o documento que orienta e estabelece as diretrizes corporativas da **Elea Data Centers** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. É cumprida e aplicada em todas as áreas da corporação.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

A política de segurança de informações foi definida com base nas necessidades de segurança exigidas pelos negócios da **Elea Data Centers**, conforme relacionado:

a. Documentada e seguida por todos os envolvidos nos processos da organização;
b. Revisada conforme necessário para se adaptar às mudanças na organização;
c. Monitorada pelos funcionários, que reportam imediatamente qualquer incidente.

Além disso, a segurança eficaz requer o planejamento e implementação de diversos controles, incluindo políticas, práticas, procedimentos e mecanismos, com responsabilidades definidas internamente.

2 Objetivo

Estabelecer diretrizes que permitam aos colaboradores, associados, clientes e prestadores de serviços da **Elea Data Centers** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa, das informações e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da **Elea Data Centers** quanto à:

1. **Confidencialidade:** assegura que a informação permaneça acessível apenas a quem deva ter acesso a respectiva informação;
2. **Integridade:** protege a exatidão e a totalidade da informação e das possíveis formas de processamento desta;
3. **Disponibilidade:** assegura que usuários autorizados tenham acesso à informação e aos ativos associados a ela quando necessário.

3 Referencias e Legislação Aplicável a Elea Data Centers

Constituição Federal;
Código de Defesa do Consumidor
Lei Federal nº 8.159, de 8 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados)
Lei Federal nº 9.610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral)
Lei Federal nº 9.279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes)
Lei Federal nº 3.129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial)
Lei Federal nº 10.406, de 10 de janeiro de 2002 (Institui o Código Civil)
Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Institui o Código Penal)
Lei Federal nº 9.983, de 14 de julho de 2000 (Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940: – Código Penal e dá outras providencias.
Lei nº 12.965, de 23 de abril de 2014 (Lei do Marco Civil da Internet)
Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)
Lei Anticorrupção (Lei Nº 12.846, de 1º de agosto de 2013)
Lei nº 10.097/2000 e Decreto nº 9.579, de 22 de novembro de 2018, relativa à Lei da Aprendizagem e de empregabilidade de menores;
ABNT NBR ISO/IEC 27001:2022;
ABNT NBR ISO/IEC 27002:2022.

4 Definições

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

- ✓ **Aceitação de risco:** decisão de aceitar um risco.
- ✓ **Áreas críticas**: dependências da **Elea Data Centers** ou de seus clientes onde esteja situado um ativo de informação relacionado a informações críticas para os negócios da empresa ou de seus clientes.
- ✓ **Ameaça:** causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou organização.
- ✓ **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco.
- ✓ **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- ✓ **Ação corretiva:** ação para eliminar a causa de uma não conformidade identificada ou outra situação indesejável.
- ✓ **Ataque:** tentativa para destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo.
- ✓ **Ativo:** qualquer componente, recurso ou conjunto destes aplicáveis para a preservação da confidencialidade, integridade e disponibilidade de dados e informações (hardware, software, infraestrutura, pessoas com seus conhecimentos etc.).
- ✓ **Ativo da informação:** conhecimento ou dados que tenham valor para a empresa.

- ✓ **Autenticidade:** propriedade que garante a autoria de um determinado dado.
- ✓ **CGSI:** Comitê Gestor de Segurança da Informação, grupo multidisciplinar que reúne representantes de diversas áreas da empresa, aprovado pela Diretoria, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção do SGSI – Sistema de Gestão de Segurança da Informação.
- ✓ **Comunicação de risco:** troca ou compartilhamento de informações sobre riscos entre o tomador de decisões e outras partes interessadas.
- ✓ **Confiabilidade:** característica de comportamento consistente e resultados desejados.
- ✓ **Confidencialidade:** característica de informação não está disponível nem pode ser revelada a indivíduos, entidades ou processos não autorizados.
- ✓ **Controle:** meios de gerenciamento de risco, incluindo políticas, procedimentos, guias, práticas ou estruturas organizacionais, que podem ser administrativos, técnicos, de gestão ou de natureza legal.
- ✓ **Controle de acesso:** meios para assegurar que o acesso a ativos é autorizado e restrito com base nos requisitos de segurança e de negócios.
- ✓ **Critérios de risco:** termos de referência pelos quais é avaliada a importância do risco.
- ✓ **Dados pessoais**: quaisquer informações associadas a uma pessoa física identificada ou identificável fornecidas pela **Elea Data Centers** e/ou acessadas em seu nome e/ou que se relacionem à condição de pessoa física vinculada à **Elea Data Centers**, incluindo, mas não se limitando a, nome, endereço, telefone, *e-mail*, dados bancários.
- ✓ **Dados sensíveis**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- ✓ **Declaração de aplicabilidade:** declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da empresa.
    - *Nota: os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, nos requisitos legais ou regulamentares, nas obrigações contratuais e nos requisitos de negócio da empresa para a segurança da informação.*
- ✓ **Disponibilidade:** característica do que é acessível e utilizável sob demanda por uma entidade autorizada.
- ✓ **Evento de segurança da informação:** uma ocorrência identificada de um estado de sistema, serviço ou rede indicando uma possível violação da Política de Segurança da Informação e Privacidade ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- ✓ **Gestão de riscos:** atividades coordenadas para direcionar e controlar uma empresa no que se refere a riscos.

- ✓ **Informações críticas para os negócios da Elea Data Centers**: toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais e/ou financeiras à **Elea Data Centers** ou seus clientes. Exemplo: dados dos clientes, fontes de sistema, regras de negócios, informações estratégias ou de negócio de clientes obtida em reuniões, planejamento estratégico da **Elea Data Centers**, prospecções, informações estratégicas da **Elea Data Centers;**
- ✓ **Incidente de segurança da informação:** um único evento ou uma série de eventos de segurança da informação indesejados ou inesperados que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- ✓ **Integridade:** propriedade de salvaguarda da exatidão e completeza dos ativos.
- ✓ **Mitigação:** limitação das consequências negativas de um determinado evento.
- ✓ **Não repúdio:** capacidade de provar a ocorrência de um evento alegado ou de ação e de suas entidades de origem, a fim de resolver disputas sobre a ocorrência ou não ocorrência de evento ou ação e envolvimento de entidades no evento.
- ✓ **Risco:** combinação da probabilidade de um evento e suas consequências.
- ✓ **Risco de segurança da Informação:** possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à empresa.
- ✓ **Risco residual:** risco remanescente após o tratamento de riscos.
- ✓ **Segurança da informação:** preservação da confidencialidade, integridade e disponibilidade da informação.
    - *Nota: adicionalmente, outras propriedades, tais como a autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.*
- ✓ **Sistema de gestão:** estrutura de políticas, procedimentos, guias e recursos associados para atingir os objetivos da empresa.
- ✓ **Sistema de Gestão da Segurança da Informação – SGSI:** parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.
- ✓ **Tratamento do risco:** processo de seleção e implementação de medidas para modificar um risco.
- ✓ **Vulnerabilidade:** fraqueza de um ativo ou controle que pode ser explorada por uma ameaça.

5 Aplicação, divulgação e Atualização

Este documento aplica-se a todas os colaboradores das áreas corporativas da **Elea Data Centers**, estagiários, prestadores de serviços, visitantes, fornecedores e temporários.

O processo de divulgação da **Política de Segurança da Informação**, está de acordo com os processos já adotados pela **Elea Data Centers** na divulgação de outros documentos e políticas. A atualização, análise crítica e revisão se dará obrigatoriamente em toda análise anual através de auditorias internas, externas ou qualquer demanda de melhoria que possa surgir ou ser identificada como necessária. Os envolvidos na implementação da Política de Segurança da Informação, incluindo a alta gerência, funcionários e terceiros, devem entender, conscientizar-se e comprometer-se com o conteúdo da política da **Elea Data Centers**.

Deverá constar em todos os contratos da **Elea Data Centers** a Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela corporação, além disso colaboradores, prestadores de serviços e parceiros assinam termo de responsabilidade.

6 Uso de Recurso corporativo

O uso de recursos de tecnologia da informação disponibilizados pela **Elea Data Centers** tais como computadores, laptops, e-mail, sistemas, Internet, bem como fornecidos por terceiros, no uso e atribuições da **Elea Data Centers**, utilizados estritamente para uso profissional e no interesse da **Elea Data Centers**, conforme documentado internamente.

O incidente que afete a segurança da informação deverá ser comunicado inicialmente à Segurança da Informação/TI e ela, se julgar necessário, deverá encaminhar as partes interessadas.

Um plano de contingência e a continuidade dos principais sistemas e serviços são implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade, disponibilidade dos ativos de informação.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a corporação julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela **Elea Data Centers** ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A **Elea Data Centers** exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, associados, clientes e prestadores de serviços reservando-se o direito

de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI foi implementada na **Elea Data Centers** por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

6.1 A palavra do Gestor

É obrigação de todos preservar a "**confidencialidade das informações**" de forma que se garanta o sigilo quando for necessário, "**a integridade**" de maneira que as informações estejam sempre corretas e a "**disponibilidade**" para que sempre que um usuário precise de uma informação, os sistemas estejam em perfeitas condições para atendê-lo.
Em virtude destes fatores a **Elea Data Centers** investe em recursos e padrões tecnológicos a fim de aumentar e melhorar a produtividade corporativa e de seus colaboradores, com objetivo de manter estes recursos foi elaborada uma **Política de Segurança da Informação**, que atende aos pré-requisitos do bom uso dos recursos computacionais desta organização.
Desta forma, problemas como vírus de computador, perda de performance, indisponibilidade de equipamentos e a necessidade de proteger a informação passam a ser tratados objetivamente, de forma a se obter os melhores resultados.
Desejo a todos que façam bom uso dos equipamentos e recursos corporativos, de maneira que a tecnologia da informação continue sendo uma ferramenta de evolução da **Elea Data Centers**.

Alessandro Lombardi
Presidente
Elea Data Centers

7 Papéis E Responsabilidades

Define-se como necessária a classificação da informação que seja de propriedade da **Elea Data Centers** ou que estejam sob sua custódia, de maneira proporcional ao seu valor para a empresa, para possibilitar o controle adequado.

7.1 Alta Direção

A Alta Direção da **Elea Data Centers** está comprometida com o sistema de gestão de segurança da informação e privacidade devendo:

1. Estabelecer as responsabilidades e atribuições para o funcionamento do SGSI;
2. Assegurar que a política e os objetivos de segurança da informação sejam estabelecidos de forma compatível com a orientação estratégica da **Elea Data Centers**;
3. Promover a integração dos requisitos do sistema de gestão de segurança da informação aos processos da **Elea Data Centers**;
4. Providenciar para que os recursos necessários para o sistema de gestão de segurança da informação estejam disponíveis;
5. Comunicar a importância da gestão eficaz da segurança da informação e do cumprimento dos requisitos do sistema de gestão da segurança da informação e privacidade;
6. Certificar que o sistema de gestão de segurança da informação alcance seus resultados pretendidos;
7. Coordenar e incentivar as pessoas a contribuírem com a eficácia do sistema de gestão da segurança da informação e privacidade;
8. Promover a melhoria contínua deste SGSI; e
9. Apoiar outras funções relevantes de gerenciamento quando demonstrem sua liderança e como ela se aplica às suas áreas de responsabilidade.
10. Analisar criticamente, juntamente com a segurança da informação os registros e resultados das auditorias realizadas na **Elea Data Centers**, incluindo o status de suas ações corretivas, listadas abaixo.

7.2 Área de TI e Segurança da Informação

Cabe as áreas:

1. Desenvolver, implementar e manter as determinações da Política de Segurança da Informação.
2. Coordenar a execução, mobilizando colaboradores para o cumprimento da Política de Segurança da Informação.
3. Promover cultura de segurança da informação.
4. Promover constantemente a cultura de segurança da informação para a organização;
5. Consolidar e coordenar a implantação, execução, monitoramento e melhoria do SGSI;
6. Convocar, coordenar e prover apoio às reuniões;
7. Prover, quando solicitado, as informações de gestão de segurança da informação que estejam sendo tratadas;
8. Coordenar as reuniões de análise crítica do SGSI e acompanhar os planos de ação resultantes delas;
9. Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;

10. Efetuar auditorias e inspeções de conformidade periódicas, bem como avaliar a eficácia, acompanhar o atendimento dos respectivos planos de ação e promover a melhoria contínua;
11. Desenvolver junto a área de Gestão de Pessoas um programa de treinamento para os colaboradores e contratados de forma a conscientizar sobre as responsabilidades de cada um em relação à segurança da informação;
12. Informar todos os colaboradores e contratados sobre a importância da Segurança da Informação e a necessidade de seguir a Política, as Normas e os Procedimentos referentes ao Sistema de Gestão de Segurança da Informação (SGSI);
13. Receber notificações de incidentes de segurança, investigar, analisar e documentar as violações e respectivas ações;
14. Estabelecer junto a Alta Direção normas e procedimentos referentes à obrigatoriedade de divulgação dos eventos e incidentes de segurança por todos os colaboradores, bem como as respectivas penalidades pelo não cumprimento desse objetivo.
15. Garantir que códigos maliciosos sejam investigados, tratados e protegidos pela ferramenta corporativa adotada pela empresa;
16. Controlar e monitorar qualquer tipo de acesso à internet fornecido pela **Elea Data Centers**
17. Assegurar o pleno e efetivo funcionamento dos recursos de tecnologia da informação disponibilizados;
18. Assegurar a integridade e disponibilidade dos ativos que se encontram no ambiente computacional;
19. Dar assistência ao gerente de TI na elaboração de normas e procedimentos de
20. Segurança da Informação, no tocante às informações, comunicações e processos relativos presentes no ambiente computacional;
21. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente;
22. Instalar e configurar as proteções necessárias (antivírus, firewall pessoal, etc);
23. Determinar quais softwares podem ou não ser instalados;
24. Realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;
25. Gerenciamento de Rede/Firewall;
26. Entre outras atividades;

8 Diretrizes

8.1 Objetivos da Gestão da Segurança da Informação

A Gestão da Segurança da Informação visa proteger as informações e a propriedade intelectual da organização, focando em:

1. Reduzir impactos de eventos de segurança, com base na Política de Segurança da Informação.
2. Identificar e monitorar riscos, com responsabilidade atribuída à diretoria de operações e colaboradores.
3. Disseminar normas e diretrizes de segurança a todos os envolvidos com a organização.

As políticas e procedimentos são revisados anualmente ou quando há mudanças significativas no negócio ou na legislação, assegurando a eficácia dos controles, que podem ser confirmados por auditorias internas.

A priorização das ações de segurança da informação deve estar alinhada com as necessidades da organização de acordo com a relevância dos processos de negócio associados.

A proteção das informações da **Elea Data Centers** é crucial e envolve as seguintes diretrizes para colaboradores, estagiários, aprendizes e prestadores de serviços:

1. Postura Proativa: Todos devem proteger as informações da empresa e estar atentos a ameaças externas e fraudes.
2. Confidencialidade: Informações confidenciais não devem ser expostas publicamente.
3. Segurança de Recursos Pessoais: Senhas e chaves são intransferíveis e não devem ser compartilhadas.
4. Software: Apenas softwares homologados podem ser utilizados.
5. Armazenamento e Descarte: Documentos confidenciais devem ser armazenados e descartados de acordo com a legislação.
6. Backup de Dados: Dados essenciais devem ter cópias de segurança e testes periódicos de recuperação.
7. Controle de Acesso Físico: Acesso às dependências deve garantir integridade, confidencialidade e disponibilidade da informação.
8. Controle de Acesso Lógico: Acesso a sistemas deve respeitar os princípios de segurança e garantir rastreabilidade.
9. Propriedade Intelectual: Criações desenvolvidas durante o vínculo com a empresa são propriedade da **Elea Data Centers**.
10. Proibição de Gravações: Equipamentos de gravação são proibidos nas dependências, salvo autorização da alta direção.
11. Impressoras: Instalação e uso de impressoras devem ser autorizados pela alta direção.
12. Uso de Computadores: Computadores da empresa devem ser usados exclusivamente para atividades relacionadas à **Elea Data Centers**, com uso pessoal restrito.

13. Conexão de Dispositivos: Dispositivos móveis particulares não podem se conectar à rede principal sem autorização, sendo que visitantes podem usar uma rede WiFi separada.

Quanto a situações, não expressamente previstas neste documento e/ou nas demais políticas e no nosso Código de Ética e Conduta, a **Elea Data Centers** conta com o bom senso de seus funcionários e caso dúvidas permaneçam, os departamentos de TI e de RH/Gestão de Pessoas podem sempre ser contatados para tirar dúvidas por meio dos e-mails rh@piemonteholding.com e suporte.ti@eleadatacenters.com.

8.2 Contato com autoridade e grupos especiais

Os contatos como polícia e bombeiros são conhecimento pelos responsáveis que englobam o escopo do SGSI.

A **Elea Data Centers** mantém contato regular com autoridades relevantes para garantir conformidade e autorização legal de suas operações. A empresa possui uma base de conhecimento atualizada sobre legislações e referências importantes, com suporte contínuo da equipe jurídica e de segurança. Além das autoridades nacionais diretamente envolvidas, existe um documento formal que lista todas as autoridades nacionais relevantes.

8.3 Inteligência de ameaças

A **Elea Data Centers** analisa e trata em tempo hábil as vulnerabilidades/ameaças no mínimo anualmente, além disso utiliza proteções avançadas em ferramenta de aplicativos e serviços de produtividade.

8.4 Segurança da informação na Gestão de Projetos

A segurança da informação deve ser sempre considerada na gestão de projetos, conforme metodologia de gestão de projetos institucional e avaliando sempre os riscos atrelados ao projeto. Documentos relacionados: Manual de Gestão de Projetos e Gestão de Projetos.

8.5 Inventário de informações e outros ativos associados

Os ativos de informação considerados relevantes para o negócio são inventariados e mantidos atualizados.

8.6 Controle de ativos

O Controle de ativos institucionais é realizado conforme procedimento específico, e trará informações pertinentes como indicação dos proprietários, tratamento, descarte, entre outros, será uma questão obrigatória, mas não se limitando a:

- ✓ Todos os softwares e hardwares da **Elea Data Centers** devem ser inventariados e controlados pelo departamento de TI.
- ✓ Não é permitida a instalação de nenhum software sem o consentimento do departamento de TI.

- ✓ Não é permitido contratar e utilizar nenhum software para uso organizacional, na nuvem ou desktop, sem o consentimento do departamento de TI.
- ✓ Não é permitido comprar ou instalar algum equipamento ou recurso sem o consentimento do departamento de TI.
- ✓ O departamento de TI deverá ter processos para detecção de softwares instalados.
- ✓ Ativos em posse de colaboradores e fornecedores devem ser controlados. Em caso de desligamento ou encerramento de contrato, o ativo deverá ser devolvido conforme procedimento estabelecido pelo departamento de TI.
- ✓ Softwares devem possuir gestão de suas licenças e uso controlado pelo departamento de TI.
- ✓ O inventário deve ser atualizado, pelo departamento de TI, a cada aquisição ou descarte.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.
O colaborador é responsável pelos ativos de TI da **Elea Data Centers**, bem como pelas Informações que inserir em tais ativos.

8.7 Classificação da Informação

A segurança da informação na empresa é classificada em quatro níveis:

a) Público: Informação acessível a todos, incluindo clientes e fornecedores, sem causar danos à organização.

b) Interno: Informação acessível apenas a funcionários, cuja divulgação externa deve ser evitada, mesmo que não cause sérios danos.

c) Restrito: Informação acessível somente a usuários específicos ou áreas designadas; divulgação não autorizada pode causar danos graves ao negócio.

d) Confidencial: Informação acessível a usuários e parceiros; sua divulgação não autorizada pode impactar financeiramente, na imagem ou operacionalmente a organização ou seus parceiros.

8.8 Transferência de informações

- ✓ Colaboradores da **Elea Data Centers** e partes externas que tratam ou possuem acesso aos ativos da **Elea Data Centers** devem ser comunicados e estar conscientes e orientados dos requisitos de segurança da informação dos ativos, informações e dados pessoais relacionados.
- ✓ Os procedimentos estabelecidos pela **Elea Data Centers** de segurança, controle de acesso, uso de softwares e antivírus, armazenamento e término do

tratamento de dados e informações devem ser seguidas por todos os envolvidos, incluindo colaboradores e fornecedores/ terceirizados, conforme aplicável.
Acordo de Confidencialidade de dados e informações, incluindo a privacidade dos dados, são assinados, entre partes, com colaboradores internos e fornecedores/terceirizados.

8.8.1 Troca de Informações com Clientes e Fornecedores

A troca de informações com clientes ou fornecedores deve ser realizada por canais seguros.

- ✓ Adotar sempre a prática da criptografia nos canais de comunicação (e-mail, Voip, SFTP, gerenciadores de arquivos).
- ✓ Não se deve transportar informações confidenciais por canais não seguros.
- ✓ Em caso de mídias físicas devem estar dentro de envelopes e/ou caixas devidamente lacradas.
- ✓ Mídias físicas devem ser criptografadas.

8.9 Gestão de Acessos

Os tipos de sistemas que necessitam de acesso lógico deverão possuir um controle formal desde a liberação do acesso até a sua revogação.
Além disso gerenciamento e reinicialização de senha, acessos privilegiados e contas de serviço são documentados internamento na **Elea Data Centers**. Além disso é realizado análise crítica dos direitos de acesso periodicamente.

8.9.1 Perfis de Acesso / Segregação de funções

Os perfis de acesso devem ser criados para cada uma das aplicações disponíveis para que os acessos sejam padronizados e uniformes.
É de responsabilidade do departamento de Infraestrutura, junto com o Security Officer e Recursos Humanos definirem a padronização dos perfis de cada departamento.

Cada um dos sistemas deve possuir um perfil de acesso básico, o qual permite somente navegação no sistema (com informações não confidenciais e não secretas). Na impossibilidade de criação de perfis na aplicação, deve-se conceder somente o direito básico a ela.

Um critério de segregação de funções para liberação de permissões, baseado em “cargos/funções/operação”, deve ser considerado, de forma que o usuário (Colaborador, estagiário, jovem aprendiz, cliente, fornecedor) **tenha acesso somente ao indispensável para execução de sua atividade**.

8.10 Segurança da informação nas relações com fornecedores

O relacionamento com fornecedores e parceiros se dará por processos como de Compliance, Gestão de Riscos, Gestão de Projetos, Aquisições e outros.

A **Elea Data Centers** deve gerenciar os acordos com fornecedores (empresas prestadoras de serviços), visando à manutenção e o cumprimento dos controles definidos em norma.

Os riscos de segurança relativos aos fornecedores e parceiros são identificados durante o processo de avaliação do risco, conforme documentação interna.

A área de Segurança da Informação é responsável por determinar se é necessário avaliar adicionalmente os riscos relativos aos fornecedores ou parceiros individuais.

8.10.1 Acesso Remoto para fornecedores

O acesso é liberado de forma pontual (suporte) e com acompanhamento de um técnico de suporte **Elea Data Centers**, devendo ser desativado o acesso ao término do atendimento.

8.10.2 Gerenciamento de Mudanças para Serviços com Fornecedores

As mudanças nos serviços prestados devem ser gerenciadas pelos responsáveis contratantes, considerando a criticidade dos sistemas e os processos de negócio envolvidos durante as atividades.

8.10.3 Gerenciamento e Monitoração dos Níveis de Serviço

O responsável pelo fornecedor deverá realizar uma análise crítica do serviço entregue, garantindo que os controles de segurança, as definições de serviço e os níveis de entrega estejam de acordo com o que foi previamente estabelecido em contrato.

8.10.4 Segurança da informação para uso de serviços em nuvem

A **Elea Data Centers** possui diretrizes de Segurança da Informação para a computação em nuvem que tem por objetivo orientar seus colaboradores a buscar a melhoria contínua nas atividades relacionadas ao planejamento, execução, análise dos seus processos/produtos, proteção da segurança das informações geradas e o correto funcionamento do Sistema de Gestão da Segurança da Informação (SGSI).

8.10.5 Gestão de Incidentes

A **Elea Data Centers** estabelece regras para Gestão de Incidentes de Segurança da Informação para:

- ✓ Garantir a detecção de eventos e tratamento adequado, sobretudo na categorização destes como incidentes de segurança da informação ou não.
- ✓ Garantir que incidentes de segurança da informação sejam identificados, avaliados e respondidos de maneira mais adequada possível.
- ✓ Minimizar os efeitos adversos de incidentes de segurança da informação (tratando-os o mais brevemente possível).
- ✓ Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente.

- ✓ Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas (Base de Conhecimento – Erros Conhecidos e tratativas de incidentes ou problemas).

O Planejamento do Processo de Gestão de Incidentes de Segurança da Informação visa que incidentes de segurança sejam sanados rapidamente.

Dependendo da severidade do incidente de segurança, o time de resposta a incidente de segurança da informação poderá decidir se o incidente reportado será tratado de forma imediata ou não. Os papéis e responsabilidades relacionados ao gerenciamento de incidentes de segurança da informação estão identificados.

Todo tratamento de incidente gerado por problema, deverá ser registrado na base de Conhecimento para se ter um histórico de tratativas, ações a respeito de incidentes de Segurança da Informação.

8.10.6 Coleta de Evidências

As evidências que comprovam o incidente devem ser coletadas tão logo seja possível. Essas evidências devem ser armazenadas em local seguro.

8.11 Prevenção de Ataques

A segurança da infraestrutura e sistemas é continuamente reavaliada para manter um nível mínimo de proteção, com foco nas soluções. O monitoramento e registro de eventos devem permitir a detecção precoce de atividades anormais e a geração oportuna de relatórios.

Medidas preventivas, detectivas e corretivas, como a aplicação de patches de segurança e controles contra malwares (vírus, *Worms, Spyware, Phishing, spam*), devem ser estabelecidas e monitoradas regularmente, implementadas conforme necessário e de acordo com as normas.

Os incidentes de segurança devem ser identificados, classificados, comunicados e tratados conforme a Norma de Gestão de Incidentes, com preservação das evidências do tratamento.

8.12 Segurança da Informação durante uma disrupção - Gestão de continuidade e disponibilidade

Para a manutenção da continuidade das atividades da **Elea Data Centers** em casos de crises, incidentes ou desastres, foi definido documentos específicos com procedimentos a serem seguidos em casos de disrupções específicas relacionadas a riscos significativos para o Sistema de Gestão de Segurança da Informação.

8.13 Propriedade Intelectual

São de propriedade da **Elea Data Centers** todos os projetos, criações, produtos e inovações levantadas e desenvolvidas internamente ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício. Além de toda informação recebida, gerada, armazenada, processada, transmitida e descartada em decorrência das operações da **Elea Data Centers** são de propriedade da organização. É vedado o armazenamento, a cópia, o uso e a transmissão de informações de propriedade intelectual ou industrial sem a autorização expressa da organização (proprietária).

8.14 Registros de eventos e log´s

Os sistemas e recursos principais da empresa (principalmente em relação a sistemas e recursos) terão log´s registrados e consultáveis, independente se de usuários comuns ou administradores.

8.15 Proteção de Registros, Proteção de Privacidade e Dados Pessoais

A capacidade de armazenamento dos eventos deve ser avaliada e integrada à gestão dos ativos. O acesso às trilhas de auditoria deve ser restrito às pessoas cuja função justifique a necessidade.

Os arquivos das trilhas de auditoria, gerenciados pelo TI, devem ser protegidos contra alterações não autorizadas com controles de acesso e cópias de segurança periódicas. Provedores de serviços em nuvem devem permitir a exportação ou cópia desses arquivos para garantir a segurança.

Exclusões de trilhas de auditoria devem ser notificadas, registradas e enviadas para a área de Segurança da Informação para garantir a integridade.

Dados importantes devem ser protegidos adequadamente, e as documentações de segurança não devem ser compartilhadas desnecessariamente. O sistema DLP (Data Loss Prevention) é utilizado para monitorar, alertar e prevenir a saída de informações confidenciais.

8.16 Análise crítica independente da segurança da informação

A avaliação e análise do material final da auditoria é realizado através de uma análise crítica dos Diretores, onde é apresentado a metodologia utilizada, as evidências coletadas, detalhamento dos pontos de não conformidades identificadas, apresentação dos pontos de melhoria identificado e a sugestão de um plano de ação.

9 Diretrizes para a segurança de controles de pessoas

9.1 Seleção

O processo de recrutamento é realizado de forma rotineira para a alimentação do banco de talentos, otimizando as atividades da área de recursos humanos para os casos de contratação em caráter de urgência.

No processo seletivo é considerado requisitos para cada vaga.

9.2 Termos e condições de contratação

Cada candidato contratado na **Elea Data Centers** é admitido, ambientado, integrado à empresa e recebe uma orientação sobre seu trabalho, conforme documentações internas, além da obrigatoriedade da assinatura de termos.

9.3 Treinamento e Conscientização do SGSI

Os colaboradores são constantemente treinados sobre o tratamento de informações e segurança, incluindo campanhas de conscientização e divulgações para elevar os padrões de segurança. O objetivo é garantir que os acesso aos ativos e informações da **Elea Data Centers** tenham conhecimento adequado e responsabilidade para proteger os dados, minimizar danos e reduzir prejuízos.

9.4 Processos disciplinares

A **Elea Data Centers** estabelece medidas disciplinares quando as Políticas, Procedimentos e Diretrizes não são cumpridas. A definição da política de sanção disciplinares foi estabelecida e assim como esta Política de Segurança da Informação faz parte das responsabilidades de trabalho dos colaboradores e prestadores de serviços. Dessa forma, o não cumprimento dela serão avaliados de acordo com a Política de Medidas Disciplinares.

9.5 Responsabilidades após encerramento ou mudança da contratação

A área de Recursos Humanos gerencia o desligamento e mudanças de contratação dos colaboradores, com algumas etapas envolvendo outras áreas e requisições do RH.

A revogação de acessos pode ocorrer em casos de desligamento, mudança de função, encerramento de contrato com fornecedores ou outras solicitações. A TI deve manter registros de acesso atualizados para garantir a exclusão ou inativação imediata dos acessos quando necessário.

O acesso de colaboradores, estagiários ou jovens aprendizes desligados é bloqueado conforme o Processo de Recrutamento e Seleção do RH. Em casos críticos, uma requisição emergencial pode ser aberta para remover o acesso em minutos.

9.6 Trabalho remoto

Procedimentos e processos que apoiam a segurança da informação foram implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto, para tal a **Elea Data Centers** autoriza seus colaboradores a realizarem o trabalho remoto (a depender da área), porém, para ter acesso a dados e recursos, os colaboradores assinam termos e responsabilidades institucionais para evitar o mal uso de recursos, bem como a habilitação de log´s e controle transacional por usuário será aplicada para evitar ações indevidas.

Acessos dos usuários podem ser auditados.

9.7 Relato de eventos de segurança da informação

A detecção, comunicação e registro de incidentes de segurança da informação seguem o Fluxo de Gestão de Incidentes descrito no normativo correspondente.

Colaboradores e fornecedores devem reportar imediatamente quaisquer fragilidades ou eventos que possam causar incidentes de segurança, por e-mail ou verbalmente, detalhando o incidente, data e hora, ou registrando-o conforme o processo.

Para contato direto a **Elea Data Centers** disponibiliza os meios:
- Contato telefônico (+55 21 3592-1221);
- Contato destinado a assuntos referente a recursos humanos: rh@piemonteholding.com;
- Contato destinado a segurança da informação/TI: suporte.ti@eleadatacenters.com

10 Diretrizes para a segurança de controles físicos e ambientais

10.1 Segurança Física

As instalações físicas da **Elea Data Centers**, onde estão os ativos de informação e serviços de Colocation, são seguras, com controles de acesso e proteção física adequados. Os equipamentos são protegidos contra ameaças físicas e ambientais, incluindo durante a logística.

Os controles de segurança física incluem:

1. Perímetros de Segurança: Ambientes operacionais tem barreiras físicas, segurança treinada, controle de acesso e CFTV para prevenir furtos e acessos indevidos.
2. Armazenamento e Proteção de Dados: Ambientes tem controle de acesso rigoroso, com salas individualizadas e segurança contratual.
3. Controle de Visitas: Registros e acompanhamento de visitantes são geridos através de um Sistema de Controle de Acesso e procedimentos específicos.
4. Restrições de Acesso: Regras de segurança devem ser cumpridas em ambientes restritos, como os de clientes e parceiros.
5. Proteção Contínua: Equipamentos e dados devem ser protegidos, inclusive em ambientes externos, com medidas como senhas, bloqueios, criptografia e antivírus.

10.2 Norma de Mesa e Tela Limpa

Todos os colaboradores, terceirizados, estagiários e jovens aprendizes da **Elea Data Centers** devem seguir as diretrizes da Política de Mesa Limpa e Tela Limpa para proteger dados e ativos, tanto digitais quanto físicos. As principais orientações são:

- ✓ Cuidados com Ativos: Utilizar e preservar os ativos com atenção.
- ✓ Bloqueio de Estações de Trabalho: Bloquear as estações ao se afastar.
- ✓ Armazenamento de Documentos: Não deixar documentos impressos na mesa; armazená-los em locais seguros.
- ✓ Segurança de Chaves: Não deixar chaves em locais acessíveis.
- ✓ Proteção de Documentos Sensíveis: Guardar documentos sensíveis em locais seguros e não os deixar visíveis.
- ✓ Destruição de Documentos: Utilizar fragmentadoras ou empresas especializadas para destruir documentos.
- ✓ Impressão e Digitalização: Evitar imprimir desnecessariamente; retirar documentos imediatamente após a impressão ou digitalização.
- ✓ Visibilidade de Dados: Posicionar móveis para que dados confidenciais não sejam visíveis.
- ✓ Organização e Segurança: Manter o espaço de trabalho limpo e organizado, documentos guardados, e dispositivos desligados ao final do expediente.
- ✓ Reuniões: Descartar informações usadas em salas de reunião de forma adequada.
- ✓ Restrições Alimentares: Não consumir alimentos ou bebidas na estação de trabalho.

10.2.1 Manutenção de Equipamentos

As manutenções em equipamentos de processamento de informação em garantia são realizadas por técnicos credenciados pela fabricante com acompanhamento de colaboradores autorizados e responsáveis a realizar o gerenciamento do ambiente, em intervalos regulares para assegurar correções preventivas.

10.3 Descarte e reutilização de equipamentos e mídias

As mídias de armazenamento utilizadas na operação dos processos do SGSI são descartadas de forma segura e protegida, como remoção dos dados para uso por outra aplicação. O descarte de mídias pode ser feito por meio de uma empresa especializada.

Deve-se assegurar que os dados sensíveis e softwares licenciados tenham sido removidos ou gravados com segurança.

11 Diretrizes para a segurança de controles tecnológicos

11.1 Gestão de capacidade

Para garantir a qualidade dos serviços adquiridos ou oferecidos, é essencial analisar e identificar os requisitos mínimos de capacidade tecnológica, humana e física. O provedor de serviço em nuvem deve informar os limites padrões dos serviços e possibilitar ajustes se estes não atenderem às necessidades do negócio.

Antes de iniciar operações, devem ser aplicados os requisitos de capacidade identificados, com base no número de licenças e recursos necessários, conforme documentação oficial da infraestrutura. A análise e identificação dos requisitos devem ser registradas para facilitar a verificação de falhas, mitigação de problemas e para orientar futuras aquisições ou ofertas de serviços.

11.2 Antivírus

A **Elea Data Centers** deve possuir software de antivírus apropriado, para proteção contra vírus e software malicioso. O software de antivírus deve ser instalado e mantido devidamente atualizado em todas as estações de trabalho dos usuários e notebooks.

11.3 Gestão de Vulnerabilidades técnicas e auditorias

A gestão do SGSI da **Elea Data Centers** deve conduzir ações para identificar e classificar os riscos de Segurança da Informação da empresa por meio do mapeamento de vulnerabilidades, ameaças, impacto e probabilidade de ocorrência, bem como da adoção de controles que mitigam estes riscos junto aos responsáveis pelos ativos aos quais os riscos estão associados.
Periodicamente a **Elea Data Centers** poderá requerer serviços técnicos especializados (Scans de vulnerabilidade) para avaliar a aderência de práticas de segurança, aferir o nível de segurança dos sistemas de informação e aplicar correções conforme níveis de criticidade que se encontram no ambiente.

11.4 Gestão de Configuração

A **Elea Data Centers** usa o processo de Gerenciamento de Itens de Configuração para controlar IC´s necessários para sua prestação serviços, para garantir que informações precisas e confiáveis sobre esses IC´s estejam disponíveis quando e onde for necessário.

O objetivo do Gerenciamento de IC´s é fornecer informações seguras e atualizadas sobre os IC´s em uso na **Elea Data Centers.**

11.5 Exclusão de Informações

A **Elea Data Centers** tem procedimentos específicos para a destruição segura de dados em papel, discos rígidos e dispositivos móveis. Esses procedimentos visam eliminar dados sensíveis de forma segura para prevenir acessos não autorizados e vazamentos. Métodos como destruição física ou sobrescrita de dados são utilizados para garantir que as informações não possam ser recuperadas. Registros das atividades de exclusão e auditorias periódicas são mantidos para assegurar a conformidade. A conscientização e o treinamento dos funcionários sobre essas práticas são essenciais para proteger a confidencialidade e integridade das informações, atendendo às exigências legais e regulamentares.

11.6 Mascaramento de dados

A **Elea Data Centers** possui procedimentos estabelecidos, específicos para o mascaramento de dados, sendo uma das técnicas utilizadas para a proteção de informações sensíveis.

11.7 Backup (Cópia de Segurança dos Dados) e *Restore*

O departamento de TI é responsável por realizar cópias de segurança (Backup) conforme os procedimentos internos para garantir a integridade dos sistemas e dados. Assegura-se que:

- ✓ Aplicações e dados tenham backups periódicos.
- ✓ Backups sejam armazenados em locais distintos do ambiente de produção.
- ✓ Backups em mídias físicas sejam criptografados.
- ✓ Backups sejam testados regularmente a cada 6 meses ou imediatamente após mudanças no ambiente.

11.8 Redundância dos recursos de processamento de informações

Os recursos de processamento de informação devem ser estruturados de maneira a garantir sua redundância e assegurar o nível de disponibilidade necessário. Em complemento a disponibilidade, considerações sobre a integridade e confidencialidade das informações devem ser adotadas para os recursos redundantes. A **Elea Data Centers** assegura a disponibilidade dos seus recursos.

11.9 Geração de Trilhas de Auditoria (LOGS) das transações efetuadas

O acesso aos ativos que afetam o ambiente de produção da **Elea Data Centers** é registrado. O provedor de serviços em nuvem possui ferramenta que possibilite a visualização dos eventos dos softwares como serviço (SaaS), ou qualquer outra solução.

11.10 Restrição de acesso à informação

A documentação dos sistemas deve ser protegida contra acessos não autorizados, definindo os locais apropriados para seu armazenamento e restringindo o número de pessoas que tem acesso a essa documentação. Essa diretriz é reforçada pelos documentos internos.

11.11 Atividades de monitoramento

Métodos de monitoramento dos ativos são estabelecidos, utilizando ferramentas automáticas sempre que possível, ou manuais, para mitigar riscos e garantir a disponibilidade dos serviços. Esses métodos são configurados para coletar informações adequadas e gerar evidências para a gestão de incidentes.

O provedor de serviços em nuvem deve ter ferramentas para analisar a qualidade dos serviços prestados. Além disso, a área de TI deve implementar monitoramento interno para assegurar que o provedor cumpra com os níveis de serviço contratados. Os

procedimentos e configurações para monitoramento estão documentados na ferramenta oficial da área de infraestrutura.

11.12 Sincronização de Relógios

Aplicativos, servidores, acesso físico e recursos deverão ter seu relógio sincronizado com AD (Active Diretory), no intuito de manter o bom funcionamento das aplicações e facilitar as investigações relacionadas a incidentes de segurança.
Caso não seja possível sincronizar com AD, o departamento de TI, poderá adotar outro canal seguro para efetuar a sincronização.

11.13 Softwares ilegais e direito autoral

A **Elea Data Centers** respeita os direitos autorais dos softwares, não permitindo o uso de softwares não licenciados. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) e os usuários não têm permissão para instalá-los, sendo necessário contatar o departamento de TI para qualquer tipo de instalação (mesmo que sejam softwares que precisem apenas ser copiados e executados).

Periodicamente, o departamento de TI fará inspeção nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta política. Caso sejam encontrados softwares não autorizados, estes deverão ser removidos dos computadores. Aqueles que instalarem em seus computadores de trabalho tais softwares não autorizados se responsabilizam perante a **Elea Data Centers** por quaisquer problemas ou prejuízos causados em decorrência de tal ato.

O departamento de TI mantém as evidências da propriedade de licenças de uso de software e registros do uso adequado do número de licenças garantindo os direitos de propriedade intelectual. Este item é aplicado conforme item **Controle de Ativos** deste **Manual de Segurança da Informação** e respectivos procedimentos.

A **Elea Data Centers** também não executa cópia de todo ou partes de livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral e sem a devida citação das referências cabíveis.

Ações disciplinares podem ocorrer na violação deste item e serão aplicadas pelo CGSI conforme o item **Sanções** desta **Manual de Segurança da Informação**.

11.14 Segurança de Redes

O acesso aos componentes da infraestrutura de produção ou qualquer outra solução sob à gestão da área de infraestrutura cloud deve ser feito utilizando mecanismo de autenticação com usuário individual e senha forte.

No caso de acesso através de rede sem fio (wireless) deve ser utilizado no mínimo o padrão de autenticação e criptografia WPA2.

11.15 Segregação de Redes

Os ambientes da **Elea Data Centers** são segregados através de tecnologia de rede VLAN (Rede de Área Local Virtual) quando aplicável, separando uma única rede comutada para atender aos requisitos funcionais e de segurança de seus sistemas.
Considerando que a maior parte de nossos colaboradores trabalham nos Data Center, as informações e aplicações utilizadas pela **Elea Data Centers** estão em servidores na nuvem, com proteção de Firewall implementada em software para abrangência de todos os equipamentos utilizados tanto internamente, no escritório, quanto externamente.

Não é permitido o acesso à rede Wireless principal ou cabeada por visitantes. Caso haja necessidade de conexão, deve ser disponibilizado acesso apenas a rede configurada para visitantes. A gestão de acesso a redes visa implementar controles para a criação, manutenção e revogação de acessos e permissões ao ambiente computacional da **Elea Data Centers**, e deve seguir as seguintes recomendações:

- ✓ Somente a área de Tecnologia da Informação está autorizada a criar, alterar e revogar acessos e/ou permissões dos sistemas, bem como ferramentas corporativas em produção.
- ✓ Os comunicados de admissão, afastamento, férias, movimentação ou desligamento de profissionais, estagiários ou menores aprendizes devem ser encaminhados à área de Tecnologia da Informação através da área de Recursos Humanos/Jurídico, via e-mail.

11.15.1 Estações e Servidores

- ✓ Estações de trabalho e servidores deverão ter controle de sessão inativa. O bloqueio deverá ser feito automaticamente após um período de inatividade determinado por TI.
- ✓ Estações de trabalho e servidores deverão possuir antivírus instalados e atualizados, e não podem ser desabilitados por usuários comuns.
- ✓ Estações de trabalho deverão possuir acesso por meio do AD.
- ✓ Acesso à porta USB estará habilitado apenas para leitura em caso de necessidade de escrita o colaborador deverá justificar ao gestor responsável, que avaliará a possibilidade.
- ✓ Informações confidenciais deverão ser armazenadas criptografadas. Estações de trabalho e Notebooks deverão ter seu HD criptografado.
- ✓ Não é permitido o compartilhamento de pastas nos computadores de colaboradores da **Elea Data Centers**. Os dados devem sempre estar no drive de rede (SharePoint ou OneDrive Corporativo) e os que necessitam de compartilhamento entre colaboradores devem ser alocados em pastas apropriadas atentando-se às permissões de acesso aplicáveis aos referidos dados.

11.15.2 Navegação na Internet

Considera-se a Internet meio essencial para busca de informações e produtividade do trabalho, portanto, seu uso em estações de trabalho está liberado sob monitoramento. Apesar da internet ser liberada, todos os funcionários são orientados quanto ao uso consciente para que não atrapalhe o andamento dos processos e atividades da **Elea Data Centers**.

Aleatoriamente a Segurança da Informação/Direção poderá posteriormente emitir relatórios de uso da internet e para os casos em que for caracterizado o uso excessivo em sites não relacionados aos negócios da **Elea Data Centers** o colaborador poderá ser sinalizado ou advertido individualmente, conforme termos de ética, sigilo e confidencialidade assinados.

É proibido o acesso a sites que contenham pornografia, racismo, pedofilia, jogos, violência e preconceitos em geral ou a sites que vão contra as leis vigentes.
Caso a **Elea Data Centers** julgue necessário haverá bloqueio de acesso a arquivos e sites não autorizados, que comprometam o bom funcionamento da rede ou o desempenho e a produtividade do profissional, bem como exponham a empresa e sua estrutura à riscos de segurança.

11.15.3 Correio Eletrônico (e-mail)

O correio eletrônico fornecido pela **Elea Data Centers** é um instrumento de comunicação interna e externa de conteúdo profissional relativa às atividades exercidas pelos colaboradores. As mensagens não devem comprometer a imagem da **Elea Data Centers**, não podem ser contrárias à legislação vigente e nem aos princípios éticos.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Os colaboradores são informados de que todos os *e-mails* trocados nos computadores da **Elea Data Centers** Digital por eles utilizados poderão ser rastreados e verificados.

É terminantemente proibido o envio de mensagens que:

- ✓ Contenham declarações difamatórias e linguagem ofensiva;
- ✓ Possam trazer prejuízos a outras pessoas;
- ✓ Sejam hostis e inúteis;
- ✓ Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- ✓ Possam prejudicar a imagem da **Elea Data Centers**;
- ✓ Possam prejudicar a imagem de outras empresas;
- ✓ Sejam incoerentes com as políticas da **Elea Data Centers**.
- ✓ Com informações que impliquem em violação de direito autoral;

Devem também ser seguidas as normas constantes no Código de Ética e Conduta da **Elea Data Centers**.

E-mails recebidos com informações de segurança (como avisos sobre *Phishing,* acesso ao *e-mail* em outro dispositivo, suspeita de vírus em arquivo, entre outros) devem ser encaminhados para TI.

Caso um e-mail seja enviado indevidamente para um destinatário, comprometendo a segurança da informação da **Elea Data Centers** e/ou das suas partes interessadas, deve ser feita a comunicação imediata ao e-mail lgpd@eleadatacenters.com para que sejam tomadas as ações necessárias.

O serviço de *e-mail* deve observar:

- ✓ *E-mails* deverão ser trafegados por canal seguro.
- ✓ A ferramenta de *e-mail* deverá ter recurso habilitado e controlado de AntiSpam e controle de conteúdo

11.15.4 E-mail pessoal

É permitido ao profissional acessar seu e-mail pessoal a partir da rede da **Elea Data Centers**, porém, é proibida a utilização deste para envio ou recebimento de qualquer tipo de dado, informações ou arquivos relacionados aos negócios da **Elea Data Centers** ou para transações em nome da **Elea Data Centers**.

Toda e qualquer comunicação com clientes, fornecedores e outros parceiros da **Elea Data Centers** deve ser feita, única e exclusivamente por meio do e-mail corporativo e não pelo e-mail pessoal de qualquer profissional.

11.15.5 Instant Messenger

É permitido o uso do Microsoft Teams apenas pelo login da **Elea Data Centers**;
A comunicação com clientes e fornecedores via WhatsApp deve ser feita preferencialmente pelo aplicativo instalado no computador. O uso do WhatsApp, tanto versão web quanto aplicativo, é monitorado pelo departamento de TI para acompanhar a entrada e saída de arquivos e pode ser bloqueado conforme diretrizes de segurança que estejam vigentes na **Elea Data Centers**.

A utilização desses aplicativos no computador da **Elea Data Centers** deve ser exclusivamente com contatos internos da **Elea Data Centers** ou com contatos externos (clientes e fornecedores) quando tratar de assuntos relacionados à empresa. Outros aplicativos são proibidos e, em caso de necessidade, é obrigatório contatar o CGSI.

11.15.6 Armazenamento em nuvem

É proibido o upload ou compartilhamento de documentos ou informações sobre a **Elea Data Centers** para qualquer tipo de dispositivo de armazenamento em nuvem (exemplo: Google Drive, Dropbox etc.) que não sejam os canais homologados para a empresa, que são:

- ✓ Diretórios de Repositórios (para backup e recuperação de dados em canais locais);
- ✓ Ambiente EAD que controlará materiais de treinamento;
- ✓ Ambiente ECM que controlará documentos e registros do SGSI;
- ✓ Microsoft OneDrive exclusivamente com usuário corporativo **Elea Data Centers**;
- ✓ E-mail institucional.

11.15.7 Varredura de Redes wi-fi

Política com o objetivo de mapear todas as redes wi-fi que estão disponíveis nos datacenters e categorizar como “Rede wi-fi Corporativa/Conhecida” ou Rede wi-fi Desconhecida”.

11.15.8 Filtragem Web

A **Elea Data Centers** possui uma solução de filtragem da web alinhada com suas normas e controles de segurança da informação, na qual são administradas por uma empresa terceirizada, definindo os critérios para filtrar o conteúdo da web. Esses controles são essenciais para proteger os sistemas contra comprometimentos por malware e para prevenir o acesso a recursos web não autorizados.

Isso inclui monitorar e analisar o tráfego da web e impor restrições de acesso com base em regras predefinidas, bloqueando sites maliciosos que podem conter malware ou outras ameaças de segurança bem como controlar o acesso a sites e a prevenir que usuários não autorizados acessem informações sensíveis, reduzindo o risco de violações de dados e ataques cibernéticos. Além de estar em conformidade com os requisitos regulatórios relacionados à segurança da informação.

Por meio do monitoramento de relatórios é possível analisar os padrões de uso da internet dentro da organização, ajudando a identificar atividades suspeitas ou ameaças potenciais.

11.16 Norma para o uso de Controles Criptográficos

Procedimentos para garantir a confidencialidade, integridade e disponibilidade das informações por meio da ativação de recursos de segurança da informação e configuração de canal seguro de comunicação devem ser estabelecidos e mantidos pelo departamento de TI. Esses procedimentos devem conter regras sobre o uso efetivo e adequado de controles criptográficos na proteção da informação.

Visando a garantia da integridade e da recuperação da informação, é proibida a implantação de controles criptográficos não homologados pelo departamento de TI.

11.16.1 Criptografia e Proteção de Ativos

Os dispositivos móveis são protegidos contra acesso indevido, de modo que computadores portáteis são criptografados e celulares devem ser protegidos com senha (quando aplicável).

11.16.2 Criptográficas e senhas

Backup: para acesso não possui arquivo de chave criptográfica, a chave é uma senha pessoal que poderá ser configurada no aplicativo, porém para restauração de backup é necessário chave criptográfica ou usuário com acesso (ex.: EAD, SharePoint);

Sistemas Web: o arquivo de chave criptográfica simétrica (público) e é transmitida pela web. A sua validade é definida pela entidade que a cria. E os dados trafegados usam a criptografia SSL para a conexão HTTPS.

E-mail: o arquivo de chave do e-mail é transmitido a partir da configuração do e-mail no computador; a validade é definida pela entidade que a cria e sua renovação são feitas automaticamente após o vencimento.

Sistema Operacional: senha pessoal e intransferível (em caso de descumprimento desta regra estará sujeito a sanções) digitada ao ligar o computador, além do BitLocker que é gerenciador pelo Microsoft Endpoint Manager, garantido assim controle total sobre os dados criptografados do equipamento.

11.17 Gestão de mudanças

A **Elea Data Centers** estabeleceu o procedimento de Gestão de Mudanças para registrar, classificar, avaliar e aprovar requisições de mudanças.

Quando houver a necessidade de alterações nos ambientes, não é permitido o uso de dados de produção em ambientes de homologação sem o devido tratamento dos dados e aprovação do dono da informação.

A segregação dos ambientes de desenvolvimento, teste e produção são mandatórias e importantes para reduzir o risco de modificações acidentais ou acessos não autorizados aos sistemas operacionais e aos dados do negócio.

11.17.1 Análise Crítica de Conformidade Técnica

A **Elea Data Centers** efetua a verificação e análise crítica de conformidade técnica.

Se aplicável e viável tecnicamente, devido a possíveis riscos mapeados e levantados sobre os ativos do sistema de segurança da informação, executa teste de invasão ou avaliações de vulnerabilidades.

11.17.2 Análise crítica de operações e soluções

Os processos de controle de mudanças em sistemas são controlados e geridos conforme procedimento específico, mudanças em plataformas operacionais, patches e outros recursos relevantes sendo analisados criticamente para evitar instabilidades.

11.17.3 Instalação e Configuração Segura de Sistemas da Elea Data Centers e de Terceiros

A realização da instalação e configuração segura de sistemas de terceiros leva em conta os seguintes aspectos, mas não limitando:

- ✓ Preparação do ambiente da instalação;
- ✓ Estratégias de particionamento de disco;
- ✓ Documentação da Instalação e Configuração;
- ✓ Senhas de administrador;
- ✓ Instalação mínima privilegiando utilização de recurso computacional;
- ✓ Desativação de Serviços Não Utilizados;
- ✓ Instalação de Correções (Patches);
- ✓ Prevenção de abuso de recursos;
- ✓ Processos de validação e homologação;
- ✓ Segregação de ambientes na estrutura do cliente;
- ✓ Transferência de recursos e conhecimento;

Para softwares adquiridos de terceiros e utilizados em sistemas operacionais consideramos manter um nível de suporte contratado e metas de atendimento/entregas.

12 Exceções

Exceções a este manual serão tratadas nos procedimentos específicos sobre cada um dos tópicos aqui abordados.

13 Violações e sanções

13.1 Violações

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não sendo está uma lista exaustiva:

1. Quaisquer ações ou situações que possam expor a **Elea Data Centers** ou seus clientes à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
2. Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa da Alta Direção;
3. Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da **Elea Data Centers** ou de seus clientes;
4. Descumprir alguns dos itens estabelecidos nesta política de segurança;

5. A não comunicação imediata à diretoria ou DPO de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação que porventura um colaborador, estagiário, jovem aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

13.2 Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à Política de Segurança da Informação da **Elea Data Centers** de Ética e Conduta da **Elea Data Centers**: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal. Podem ainda ocorrer sanções definidas pelo CGSI sempre respeitando a legislação vigente.

Também serão observadas e aplicadas as penalidades previstas na Consolidação das Leis de Trabalho – CLT.

14 Anexos

N/A

15 Registros

Lista de distribuição					
Acesso público					
Distribuição	**Armazenamento**	**Preservação**	**Recuperação**	**Retenção**	**Descarte**
Eletrônica	ECM	Backup	Data e versionamento	5 anos	Registro permanente no EAD

16 Histórico de alterações

DATA	REVISÃO	ELABORAÇÃO	APROVAÇÃO	DESCRIÇÃO
26/10/2022	3.0	Antônio Mota	Comitê de Segurança da Informação	Acrescentado o item “Varredura de Redes Wi-fi” para cumprimento das exigências da norma do PCI DSS.
31/05/2023	4.0	Antônio Mota	Comitê de Segurança da Informação	Atualização do conteúdo da Norma ABNT NBR ISO/IEC 27001:2013 para Norma ABNT NBR ISO/IEC 27001:2022
16/08/2023	5.0	Antônio Mota	Comitê de Segurança da Informação	Atualização na disposição das informações no documento em questão.
04/10/2024	6.0	Laís Gedraits	Segurança da Informação, TI, Jurídico, Recursos Humanos e Alta direção.	Atualização na disposição das informações no documento, além da classificação da informação.