PL-001

Política de Segurança da Informação

ÍNDICE

1 Objetivo

A Política de Segurança da Informação (PSI) da Elea Data Centers define diretrizes para proteger os ativos de informação e reduzir riscos legais, aplicável a todos os colaboradores e áreas da organização.

Baseada nas normas ABNT NBR ISO/IEC 27001:2022 e ISO/IEC 27701:2019, a PSI assegura proteção da informação e conformidade legal.

Todos os envolvidos devem cumprir a política, que será revisada conforme mudanças na organização ou no ambiente regulatório, e reportar imediatamente qualquer incidente.

A segurança da informação e privacidade é garantida por meio de controles, procedimentos e responsabilidades claramente definidos.

2 Objetivo

Estabelecer diretrizes que orientem colaboradores, associados, clientes e prestadores de serviços da Elea Data Centers a seguir padrões de comportamento relacionados ao Sistema de Gestão Integrado, alinhados às necessidades do negócio e à proteção legal da empresa, das informações e das pessoas.

Orientar a criação de normas, procedimentos, controles e processos necessários para o atendimento ao SGI.

Preservar as informações da Elea Data Centers em termos de:

Confidencialidade: garantir que a informação seja acessível apenas a pessoas autorizadas;

Integridade: proteger a exatidão e a completude da informação e de seu processamento;

Disponibilidade: assegurar que usuários autorizados tenham acesso às informações e aos ativos relacionados sempre que necessário.

3 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;
- ✓ **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 SGI da empresa;
- ✓ **Disponibilidade:** Característica do que é acessível e utilizável sob demanda por uma entidade autorizada;
- ✓ **Evento de Sistema de Gestão Integrado:** 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 e privacidade:** 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;
- ✓ **Sistema de Gestão Integrado (SGI):** É um conjunto estruturado de políticas, processos, procedimentos e controles que permite à **Elea Data Centers** gerenciar de forma coordenada as áreas de qualidade, meio ambiente, energia, segurança da informação e demais aspectos corporativos, garantindo conformidade legal, eficiência operacional e proteção dos ativos de informação e das pessoas;
- ✓ **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.
- ✓ **EHS (Environment, Health & Safety):** refere-se ao conjunto de práticas, políticas e processos adotados por uma organização para proteger o meio ambiente, garantir a saúde e o bem-estar de colaboradores e terceiros, e prevenir acidentes, promovendo a segurança no local de trabalho.

4 Referências 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 nº 13.853, de 8 de julho de 2019 (ANPD);
- ✓ 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;
- ✓ Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho);
- ✓ ABNT NBR ISO/IEC 27001:2022;
- ✓ ABNT NBR ISO/IEC 27002:2022;
- ✓ ABNT NBR ISO/IEC 27701:2019.

5 Objetivos do SGI

O objetivo do Sistema de Gestão Integrado (SGI) da Elea Data Centers é estabelecer diretrizes e práticas que garantam a gestão eficiente e segura dos processos da organização, assegurando conformidade legal, proteção dos ativos de informação e melhoria contínua. Isso inclui a análise criteriosa de fornecedores, a investigação e identificação da causa raiz de incidentes, e a implementação de ações operacionais sustentáveis, como a substituição de equipamentos por soluções mais eficientes, promovendo eficiência energética e redução de impactos ambientais.

6 Aplicação, divulgação e Atualização

Esta política se aplica a todos os colaboradores, estagiários, prestadores de serviços, visitantes, fornecedores e temporários da Elea Data Centers.

A divulgação segue os mesmos processos utilizados para outros documentos corporativos, e a atualização ocorre anualmente, durante auditorias internas ou externas, ou sempre que identificadas oportunidades de melhoria.

Todos os envolvidos, incluindo alta gerência, funcionários e terceiros, devem compreender, conscientizar-se e comprometer-se com a política.

O acesso aos ativos de informação depende da assinatura de cláusula de confidencialidade em contratos e de termos de responsabilidade por colaboradores, prestadores de serviços e parceiros.

7 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.

Qualquer incidente que comprometa a segurança da informação deverá ser comunicado à TI e/ou ao SGI. Caso necessário, TI e/ou SGI deverão encaminhar a informação às partes interessadas.

O plano de contingência e a continuidade de cenários críticos para a empresa são implantados e testados, no mínimo, anualmente, com o objetivo de reduzir os riscos relacionados à perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

São criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, nos 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.

Os ambientes de produção são 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.

8 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

9 Papéis E Responsabilidades

Colaboradores, prestadores de serviços e terceiros que tenham acesso aos ativos de informação da empresa têm responsabilidades definidas para garantir a proteção, confidencialidade, integridade e disponibilidade das informações.

9.1 Alta Direção

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

- ✓ Estabelecer as responsabilidades e atribuições para o funcionamento do SGI;
- ✓ Assegurar que a política e os objetivos do SGI sejam estabelecidos de forma compatível com a orientação estratégica da Elea Data Centers;
- ✓ Promover a integração dos requisitos do sistema de gestão de segurança da informação e privacidade aos processos da Elea Data Centers;
- ✓ Providenciar para que os recursos necessários para o sistema de gestão de segurança da informação e privacidade estejam disponíveis;
- ✓ 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;
- ✓ Certificar que o SGI alcance seus resultados pretendidos;
- ✓ Coordenar e incentivar as pessoas a contribuírem com a eficácia do sistema de gestão da segurança da informação e privacidade;
- ✓ Promover a melhoria contínua deste SGI;
- ✓ Apoiar outras funções relevantes de gerenciamento quando demonstrem sua liderança e como ela se aplica às suas áreas de responsabilidade;
- ✓ Analisar criticamente, juntamente com o SGI os registros e resultados das auditorias realizadas na Elea Data Centers, incluindo o status de suas ações corretivas;

- ✓ Entre outras atividades;

9.2 Área de SGI

Cabe a área do SGI:

- ✓ Desenvolver, implementar e manter as determinações da Política de Segurança da Informação.
- ✓ Coordenar a execução, mobilizando colaboradores para o cumprimento da Política de Segurança da Informação e Política de Privacidade.
- ✓ Promover cultura de segurança da informação e privacidade.
- ✓ Promover constantemente a cultura de segurança da informação e privacidade para a organização;
- ✓ Consolidar e coordenar a implantação, execução, monitoramento e melhoria do SGI;
- ✓ Convocar, coordenar e prover apoio às reuniões;
- ✓ Prover, quando solicitado, as informações de gestão de segurança da informação que estejam sendo tratadas;
- ✓ Coordenar as reuniões de análise crítica do SGI e acompanhar os planos de ação resultantes delas;
- ✓ Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação e privacidade;
- ✓ 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;
- ✓ Receber notificações de incidentes de segurança, investigar, analisar e documentar as violações e respectivas ações;
- ✓ Estabelecer junto a Alta Direção normas e procedimentos referentes à obrigatoriedade de divulgação dos eventos e incidentes de segurança e privacidade por todos os colaboradores, bem como as respectivas penalidades pelo não cumprimento desse objetivo.

- ✓ Dar assistência aos gerentes na elaboração de normas e procedimentos de segurança da Informação, no tocante às informações, comunicações e processos relativos presentes no ambiente computacional;
- ✓ Entre outras atividades;

9.3 Área de TI

Cabe a área:

- ✓ Coordenar a execução, mobilizando colaboradores para o cumprimento da Política de Segurança da Informação;
- ✓ Promover cultura de segurança da informação e privacidade;
- ✓ Promover constantemente a cultura de segurança da informação para a organização;
- ✓ Consolidar e coordenar a implantação, execução, monitoramento e melhoria do SGI;
- ✓ Convocar, coordenar e prover apoio às reuniões;
- ✓ Prover, quando solicitado, as informações de gestão de segurança da informação que estejam sendo tratadas;
- ✓ Coordenar análises críticas e acompanhar os planos de ação resultantes delas, conforme demanda;
- ✓ Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;
- ✓ Desenvolver junto a área RH programa de treinamento para os colaboradores e contratados de forma a conscientizar sobre as responsabilidades de cada um em relação à segurança da informação;
- ✓ 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 Integrado (SGI), quando pertinente;

- ✓ Receber notificações de incidentes de segurança, investigar, analisar e documentar as violações e respectivas ações, além disso quando pertinente apoiar demais áreas;
- ✓ Garantir que códigos maliciosos sejam investigados, tratados e protegidos pela ferramenta corporativa adotada pela empresa;
- ✓ Controlar e monitorar qualquer tipo de acesso à internet fornecido pela **Elea Data Centers;**
- ✓ Assegurar pleno e efetivo funcionamento dos recursos de tecnologia da informação disponibilizados;
- ✓ Assegurar a integridade e disponibilidade dos ativos que se encontram no ambiente computacional;
- ✓ Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente;
- ✓ Instalar e configurar as proteções necessárias (antivírus, firewall pessoal, etc);
- ✓ Determinar quais softwares podem ou não ser instalados;
- ✓ Realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes, quando pertinente;
- ✓ Gerenciamento de Rede/Firewall;
- ✓ Entre outras atividades;

10 Diretrizes - Controles Organizacionais

10.1 Objetivos do Sistema de Gestão Integrado

O Sistema de Gestão Integrado da **Elea Data Centers** tem como objetivo proteger as informações e a propriedade intelectual da organização, assegurando a confidencialidade, integridade e disponibilidade dos ativos. Para isso, busca: avaliação de fornecedores críticos, a análise estruturada das causas de incidentes de maior impacto e a adoção de iniciativas que incentivem a eficiência energética e a responsabilidade ambiental em suas instalações.

As políticas e procedimentos de segurança são revisados periodicamente, no mínimo anualmente ou sempre que houver mudanças relevantes no negócio ou na legislação, garantindo sua eficácia e alinhamento às necessidades organizacionais. A efetividade dos controles pode ser confirmada por meio de auditorias independentes, reforçando o compromisso da **Elea Data Centers** com a segurança e a melhoria contínua.

A priorização das ações de segurança da informação é definida em alinhamento com as necessidades da organização, considerando 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 prévia;

11. **Uso de Computadores:** Computadores da empresa devem ser usados exclusivamente para atividades relacionadas à Elea Data Centers, com uso pessoal restrito;
12. **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, RH, SGI e EHS podem sempre ser contatados para tirar dúvidas por meio dos e-mails rh@piemonteholding.com, suporte.ti@eleadatacenters.com, ehs@eleadatacenters.com e sgi@eleadatacenters.com.

10.2 Contato com autoridade e grupos especiais

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

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.

10.3 Inteligência de ameaças

A **Elea Data Centers** analisa e trata vulnerabilidades e ameaças em tempo hábil, realizando avaliações no mínimo trimestralmente e sempre que necessário diante de novos riscos identificados. Além disso, emprega mecanismos de inteligência de ameaças para antecipar tendências, monitorar indicadores de comprometimento e responder de forma proativa a potenciais incidentes. Para reforçar essa atuação, são

utilizadas soluções avançadas de segurança em aplicativos e serviços de produtividade, combinadas a processos de varredura de vulnerabilidades, correção de falhas e monitoramento contínuo de logs. Complementarmente, a empresa mantém controles de proteção contra códigos maliciosos, políticas de atualização de patches, bem como auditorias e testes de segurança periódicos, assegurando a proteção dos ativos críticos e a redução de riscos relacionados à confidencialidade, integridade e disponibilidade das informações.

10.4 Segurança da informação na Gestão de Projetos

A segurança da informação é considerada na gestão de projetos, conforme metodologia de gestão de projetos institucional e avaliando sempre os riscos atrelados ao projeto, conforme documentação interna.

10.5 Inventário de informações e outros ativos associados

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

10.6 Controle de ativos

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

- ✓ Os softwares e hardwares da Elea Data Centers são inventariados e controlados pelo departamento de TI e/ou departamento Ativos;
- ✓ 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;
- ✓ Ativos em posse de colaboradores e fornecedores são controlados. Em caso de desligamento ou encerramento de contrato, o ativo deverá ser devolvido conforme procedimento estabelecido pelo departamento de TI;
- ✓ Softwares possuem gestão de suas licenças e uso controlado pelo departamento de TI;
- ✓ O inventário é atualizado, pelo departamento de TI e/ou Ativos, conforme demanda.

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.

10.7 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 sérios 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.

10.8 Transferência de informações

- ✓ Colaboradores da Elea Data Centers e/ou partes externas que tratam ou possuem acesso a ativos da organização são devidamente comunicados, orientados e conscientizados quanto aos requisitos de segurança da informação aplicáveis a ativos, informações e dados pessoais, estando também sujeitos às cláusulas previstas em Acordo de Confidencialidade assinado;
- ✓ 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 são seguidos pelos 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.

10.8.1 Estações e Servidores

- ✓ Bloqueio de Sessão: Estações de trabalho e servidores devem possuir controle de sessão inativa, com bloqueio automático configurado pelo departamento de TI após um período determinado de inatividade;
- ✓ Proteção por Antivírus: As estações de trabalho e servidores devem ter antivírus instalado e atualizado, sendo proibida a desativação por usuários comuns;
- ✓ Autenticação via AD: O acesso às estações de trabalho deve ser realizado exclusivamente por meio do Active Directory (AD), garantindo rastreabilidade e segurança;
- ✓ Controle de Portas USB: O acesso à porta USB será habilitado apenas para leitura. Para operações de escrita, o colaborador deve justificar a necessidade junto ao gestor responsável, que avaliará a autorização;
- ✓ Criptografia de Dados: Informações confidenciais devem ser armazenadas de forma criptografada. HDs de notebooks e, em algumas estações de trabalho,

também são criptografados, garantindo proteção contra acessos não autorizados;

- ✓ Compartilhamento de Dados: Não é permitido o compartilhamento de pastas nos computadores dos colaboradores. Os dados devem ser armazenados no drive de rede, e qualquer compartilhamento necessário entre colaboradores deve ocorrer em pastas designadas, com permissões de acesso adequadas.

10.8.2 Navegação na Internet

O uso da Internet é considerado essencial para a busca de informações e a produtividade no trabalho, sendo permitido em estações de trabalho, sob monitoramento constante. Os colaboradores recebem orientações sobre o uso responsável da rede, de modo a não comprometer o andamento dos processos e atividades da **Elea Data Centers.**

A área de Segurança da Informação ou a Alta Direção poderá, periodicamente, emitir relatórios de uso da Internet. Nos casos em que for identificado uso excessivo em sites não relacionados às atividades da empresa, o colaborador poderá ser advertido ou sinalizado individualmente, conforme os termos de ética, sigilo e confidencialidade assinados.

É proibido acessar sites que contenham pornografia, racismo, pedofilia, jogos, violência, preconceito ou qualquer conteúdo que viole a legislação vigente. Quando necessário, a **Elea Data Centers** poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o bom funcionamento da rede, afetem o desempenho ou produtividade do colaborador, ou exponham a empresa e sua infraestrutura a riscos de segurança.

10.8.3 Correio Eletrônico (e-mail)

O correio eletrônico fornecido pela **Elea Data Centers** é um instrumento de comunicação interna e externa, destinado exclusivamente a conteúdos profissionais

relacionados às atividades dos colaboradores. As mensagens devem respeitar a legislação vigente, os princípios éticos e não comprometer a imagem da empresa.

O uso do e-mail é pessoal, e cada usuário é responsável por todas as mensagens enviadas a partir de seu endereço. Os colaboradores estão cientes de que os e-mails trocados nos computadores da **Elea Data Centers** podem ser monitorados, rastreados e verificados, garantindo a segurança e conformidade das comunicações.

É estritamente proibido o envio de mensagens que:

- ✓ Contenham declarações difamatórias, linguagem ofensiva ou hostil;
- ✓ Possam causar prejuízos a terceiros;
- ✓ Sejam correntes, de conteúdo pornográfico ou inútil;
- ✓ Prejudiquem a imagem da **Elea Data Centers** ou de outras empresas;
- ✓ Sejam incompatíveis com as políticas internas;
- ✓ Impliquem violação de direitos autorais.

Os colaboradores seguem também as normas previstas no Código de Ética e Conduta da **Elea Data Centers**.

E-mails recebidos contendo informações de segurança, como alertas de phishing, acessos suspeitos ou arquivos com possíveis vírus, devem ser encaminhados imediatamente para o departamento de TI (Canal informado nesta política).

Caso um e-mail seja enviado indevidamente e comprometa a segurança de Dados Pessoais de titulares vinculados à **Elea Data Centers** ou de suas partes interessadas, o incidente deve ser comunicado imediatamente para lgpd@eleadatacenters.com, a fim de que sejam adotadas as medidas corretivas necessárias.

O serviço de e-mail deve ainda observar:

- ✓ Todos os e-mails devem trafegar por canal seguro;
- ✓ A ferramenta de e-mail possui recursos de segurança ativos como criptografia, além de controle de conteúdo, devidamente configurados, monitorados e atualizados.

10.8.4 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** é feita, única e exclusivamente por meio do e-mail corporativo e não pelo e-mail pessoal de qualquer profissional.

10.8.5 Instant Messenger

O uso de aplicativos de comunicação corporativa é permitido exclusivamente por meio das credenciais fornecidas pela **Elea Data Centers**. A comunicação com clientes e fornecedores deve ser realizada preferencialmente por aplicativos corporativos instalados nos computadores da empresa. O uso desses aplicativos é monitorado pelo departamento de TI, incluindo entrada e saída de arquivos, e pode ser bloqueado de acordo com as diretrizes de segurança vigentes na **Elea Data Centers**.

A utilização desses aplicativos nos computadores corporativos deve se restringir a contatos internos da **Elea Data Centers** ou a contatos externos (clientes e fornecedores) quando relacionados a assuntos profissionais. Qualquer outro aplicativo de comunicação não autorizado é proibido, e, em casos de necessidade, a utilização deve ser previamente aprovada pelo superior.

10.9 Troca de Informações com Clientes e Fornecedores

A troca de informações com clientes ou fornecedores são realizadas por canais seguros:

- ✓ Adotar sempre a prática da criptografia nos canais de comunicação (e-mail, Voip, gerenciadores de arquivos);
- ✓ Não se deve transportar informações confidenciais por canais não seguros;
- ✓ Mídias físicas devem ser criptografadas.

10.10 Gestão de Acessos

Os sistemas que requerem acesso lógico devem possuir controles formais desde a concessão até a revogação dos acessos. O gerenciamento de senhas, incluindo sua reinicialização, bem como o controle de acessos privilegiados e contas de serviço, é devidamente documentado internamente na **Elea Data Centers**. Adicionalmente, são realizadas análises críticas periódicas dos direitos de acesso, assegurando que permaneçam adequados às funções desempenhadas e alinhados às políticas de segurança da informação da organização.

10.11 Perfis de Acesso / Segregação de funções

Os perfis de acesso são criados para cada uma das aplicações disponíveis para que os acessos sejam padronizados e uniformes.

Cada um dos sistemas possui 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 (Mínimo privilégio).

10.12 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** gerencia 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.

As áreas pertinentes ao negócio são responsáveis por determinar se é necessário avaliar adicionalmente os riscos relativos aos fornecedores ou parceiros individuais.

10.12.1 Gerenciamento de Mudanças para Serviços com Fornecedores

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

10.12.2 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.

10.13 Segurança da informação para uso de serviços em nuvem

A **Elea Data Centers** adota práticas de segurança da informação para o uso de serviços em nuvem, incluindo soluções SaaS (Software as a Service). Os serviços são avaliados quanto a requisitos de proteção de dados, conformidade regulatória e controles de acesso antes de sua utilização. Os acessos são gerenciados formalmente, com autenticação segura e monitoramento contínuo de atividades, assegurando que apenas usuários autorizados possam manipular informações críticas. Além disso, são aplicadas medidas de criptografia para armazenamento e transmissão de dados, políticas de backup e continuidade, e procedimentos de monitoramento e auditoria periódica, garantindo confidencialidade, integridade e disponibilidade das informações na nuvem.

10.14 Gestão de Incidentes

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

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

Há documentações internas sobre o processo de Gestão de Incidentes do SGI.

Dependendo da severidade do incidente, 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.

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 do SGI.

10.15 Coleta de Evidências

As evidências relacionadas a eventos relevantes, sejam incidentes de segurança, falhas operacionais ou outras ocorrências críticas, são coletadas assim que possível. Essas evidências são armazenadas em local seguro, de forma a preservar sua integridade e disponibilidade, permitindo análises futuras, auditorias e ações corretivas adequadas.

10.16 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 permite a detecção precoce de atividades anormais e a geração oportuna de relatórios.

Medidas preventivas, detectivas e corretivas, como a aplicação de patches de segurança ou controles contra malwares, são estabelecidas e monitoradas regularmente, implementadas conforme necessário e de acordo com as normas.

Os incidentes de segurança e privacidade são identificados, classificados, comunicados e tratados conforme documentação interna, com preservação das evidências do tratamento.

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

Para garantir a continuidade das atividades da **Elea Data Centers** em situações de crises, incidentes ou desastres, foram definidos documentos específicos com procedimentos a serem seguidos diante de disrupções relacionadas a riscos significativos do Sistema de Gestão Integrado (SGI). Esses documentos integram o Plano de Continuidade de Negócios (PCN), contemplando cenários críticos para a empresa e para os serviços de Colocation. Os planos são periodicamente testados e atualizados, assegurando a eficácia das ações de resposta e a manutenção da disponibilidade, integridade e confidencialidade dos serviços prestados aos clientes.

10.18 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. Vedado o armazenamento, a cópia, o uso e a transmissão de informações de propriedade intelectual ou industrial sem a autorização expressa da organização (proprietária).

10.19 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.

10.20 Proteção de Registros, Proteção de Privacidade e Dados Pessoais

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

Os arquivos das trilhas de auditoria, são 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.

Dados importantes são protegidos adequadamente, e as documentações de segurança não devem ser compartilhadas desnecessariamente.

10.21 Análise crítica independente da segurança da informação

A avaliação e análise do material final da auditoria é realizado através de uma análise crítica da alta direção, 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.

11 Diretrizes - Controles de Pessoas

11.1 Seleção

A **Elea Data Centers** realiza o processo de seleção de colaboradores de forma estruturada e alinhada aos procedimentos internos da organização. Essa prática garante a escolha de profissionais que atendam aos requisitos técnicos e comportamentais necessários, contribuindo para a segurança, eficiência e conformidade das operações.

11.2 Termos e condições de contratação

Cada colaborador admitido na **Elea Data Centers** passa por um processo de ambientação e integração à empresa, recebendo orientações sobre suas atividades conforme as documentações internas. Além disso, é obrigatória a assinatura dos termos aplicáveis, assegurando ciência e compromisso com as políticas da organização.

11.3 Treinamento e Conscientização do SGI

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.

11.4 Processos disciplinares

A **Elea Data Centers** aplica medidas disciplinares sempre que houver descumprimento das Políticas, Procedimentos ou Diretrizes estabelecidas. A Política de Medidas Disciplinares integra as responsabilidades de trabalho de colaboradores

e prestadores de serviços, assim como esta Política de Segurança da Informação. Dessa forma, qualquer não conformidade será avaliada e tratada de acordo com as disposições previstas na documentação interna.

11.5 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. As áreas acionadas mantem registros.

O acesso de colaboradores, estagiários ou jovens aprendizes desligados é bloqueado conforme documentação interna. Em casos críticos, uma requisição emergencial pode ser aberta para remover o acesso imediatamente.

Os colaboradores da **Elea Data Centers** permanecem responsáveis pela confidencialidade e proteção das informações às quais tiveram acesso durante seu vínculo com a empresa, mesmo após o encerramento do contrato de trabalho. Essa obrigação está formalizada por meio dos Acordos de Confidencialidade e demais termos assinados, sendo vedada a utilização, divulgação ou compartilhamento de quaisquer dados, ativos ou informações estratégicas da organização após a saída. O descumprimento dessas responsabilidades poderá resultar em medidas legais cabíveis.

11.6 Trabalho remoto

Procedimentos e processos de segurança da informação foram implementados para proteger dados acessados, processados ou armazenados em ambientes de trabalho remoto. A **Elea Data Centers** autoriza o trabalho remoto para determinadas áreas, desde que os colaboradores cumpram os termos e responsabilidades institucionais

firmados, garantindo o uso adequado dos recursos corporativos. Para reforçar a segurança, são aplicados mecanismos de registro de logs, controles em Softwares e possibilidade de auditoria dos acessos, prevenindo e detectando ações indevidas.

11.7 Relato de eventos de segurança da informação

A detecção, comunicação e registro de incidentes do SGI seguem o Fluxo de Gestão de Incidentes definido no normativo específico.

Todos os colaboradores e fornecedores devem reportar imediatamente quaisquer fragilidades ou eventos que possam resultar em incidentes de segurança, seja por e-mail, contato telefônico ou verbalmente, informando detalhes como data, hora e descrição do ocorrido, ou ainda registrando-os conforme o processo estabelecido.

Para contato direto, a **Elea Data Centers** disponibiliza os seguintes canais, além de demais ferramentas homologadas:

- ✓ Telefone (+55 21 3592-1221): canal geral para comunicação de incidentes urgentes;
- ✓ Recursos Humanos (rh@piemonteholding.com): comunicação de incidentes relacionados a conduta, colaboradores ou prestadores de serviço;
- ✓ TI (suporte.ti@eleadatacenters.com): reporte de incidentes técnicos, falhas de sistemas, acessos indevidos ou vulnerabilidades de segurança da informação;
- ✓ SGI (sgi@eleadatacenters.com): comunicação de incidentes relacionados ao Sistema de Gestão Integrado, incluindo processos, procedimentos e controles internos;
- ✓ EHS (ehs@eleadatacenters.com): canal para reporte de incidentes relacionados a meio ambiente, saúde e segurança no trabalho, incluindo situações como ruídos excessivos nas redondezas e outras condições que possam afetar o bem-estar e a conformidade ambiental;
- ✓ Denúncias anônimas (Disponível no site da Elea Data Centers): canal para reportar de forma confidencial qualquer conduta inadequada ou incidente que requeira anonimato.

12 Diretrizes - Controles Físicos

12.1 Segurança Física

As instalações físicas da **Elea Data Centers**, que abrigam os ativos de informação e os serviços de Colocation, são projetadas para garantir segurança, com controles de acesso e proteção física adequados. Os equipamentos são protegidos contra ameaças físicas e ambientais.

Os principais controles de segurança física incluem:

- ✓ Perímetros de Segurança: Ambientes operacionais contam com barreiras físicas, equipe de segurança treinada, controle de acesso e CFTV, prevenindo furtos e acessos não autorizados;
- ✓ Armazenamento e Proteção de Dados: Salas individualizadas com controle rigoroso de acesso e segurança contratual asseguram a proteção dos dados armazenados;
- ✓ Controle de Visitas: Visitantes são registrados por meio de Sistema de Controle de Acesso e procedimentos específicos, garantindo rastreabilidade;
- ✓ Restrições de Acesso: Regras de segurança são aplicadas em ambientes restritos, incluindo áreas destinadas a clientes e parceiros;
- ✓ Proteção Contínua: Equipamentos e informações permanecem protegidos em todos os ambientes, internos e externos, por meio de senhas, bloqueios, criptografia, antivírus e outras medidas preventivas;
- ✓ Manutenção Preventiva e Corretiva: Os equipamentos críticos como UPS, Geradores, Sistema de refrigeração passam por manutenção regular, garantindo disponibilidade, confiabilidade e mitigando riscos de falhas físicas ou ambientais.

12.2 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: Documentos devem ser destruídos por meio de mecanismos adequados, como trituradores de papel ou outros métodos controlados que permitam a fragmentação manual, garantindo que as informações não possam ser recuperadas;
- ✓ Impressão e Digitalização: Evitar imprimir desnecessariamente, retirar documentos imediatamente após a impressão ou digitalização;
- ✓ 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: Evitar o consumo de alimentos ou bebidas na estação de trabalho.

12.3 Manutenção de Equipamentos

A manutenção dos equipamentos da **Elea Data Centers** como UPS, Gerador e Sistemas de Refrigerador é realizada prioritariamente pela equipe interna, garantindo conhecimento e controle sobre os ativos. Quando necessário, a execução pode ser realizada por terceiros qualificados, seguindo procedimentos definidos e autorizados pela empresa, assegurando a continuidade operacional, segurança e confiabilidade dos sistemas.

12.4 Descarte e reutilização de equipamentos e mídias

As mídias de armazenamento utilizadas nos processos do SGI são descartadas de forma segura, incluindo a remoção de dados quando a mídia será reutilizada em outra aplicação. O descarte pode ser realizado internamente ou por meio de empresas especializadas, quando necessário. É fundamental assegurar que informações sensíveis e softwares licenciados sejam devidamente apagados ou destruídos de maneira segura, prevenindo qualquer risco de acesso não autorizado. Para mídias de clientes contratados em serviços de Colocation, o descarte seguro é de responsabilidade do próprio cliente, não cabendo à **Elea Data Centers** essa execução.

13 Diretrizes - Controles Tecnológicos

13.1 Gestão de capacidade

Para garantir a qualidade dos serviços oferecidos ou contratados, é essencial analisar e identificar os requisitos mínimos de capacidade tecnológica, humana e física. No caso de serviços em nuvem, o provedor deve informar os limites padrão e possibilitar ajustes sempre que estes não atenderem às necessidades do negócio.

Antes do início das operações, são atendidos os requisitos de capacidade previamente identificados, considerando o número de licenças, recursos necessários. A **Elea Data Centers** realiza a gestão contínua da capacidade de seus Data Halls, monitorando recursos físicos, energia, refrigeração e infraestrutura, assegurando que os serviços permaneçam disponíveis, confiáveis e escaláveis conforme a demanda.

13.2 Antivírus

A **Elea Data Centers** possui software de antivírus apropriado, para proteção contra vírus e software malicioso. O software de antivírus é instalado e mantido devidamente atualizado nas estações de trabalho dos usuários (Quando aplicável) e notebooks.

13.3 Gestão de Vulnerabilidades técnicas e auditorias

A TI e/ou o SGI, conforme o contexto e a situação, conduzem ações para identificar e classificar os riscos relacionados à Segurança da Informação na Elea Data Centers. Esse processo envolve o mapeamento de vulnerabilidades, ameaças, impactos e a probabilidade de ocorrência, bem como a definição e implementação de controles mitigatórios em conjunto com os responsáveis pelos ativos aos quais os riscos estão associados. Quando necessário, ambas as áreas podem solicitar suporte das demais áreas da empresa para assegurar a efetividade das ações de mitigação.

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.

13.4 Gestão de Configuração

A **Elea Data Centers** utiliza o processo de Gerenciamento de Itens de Configuração (ICs) para controlar os ativos necessários à prestação de seus serviços, garantindo que informações precisas e confiáveis sobre esses itens estejam disponíveis sempre que necessário. O objetivo desse processo é fornecer dados seguros, atualizados e completos sobre os ICs em uso, apoiando a operação eficiente e a tomada de decisão dentro da organização.

13.5 Exclusão de Informações

A **Elea Data Centers** possui procedimentos específicos para a destruição segura de dados em papel e dispositivos móveis, visando eliminar informações sensíveis e prevenir acessos não autorizados ou vazamentos. São utilizados métodos como destruição física ou exclusão dados lógicos, garantindo que as informações não possam ser recuperadas. 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.

Para mídias pertencentes a clientes de serviços de Colocation, a exclusão segura é de responsabilidade do próprio cliente, não cabendo à **Elea Data Centers** realizar essa operação.

13.6 Mascaramento de dados

A **Elea Data Centers** possui documentação estabelecidos para o mascaramento de dados, realizado por meio da criptografia nativa dos softwares utilizados, garantindo a proteção de informações sensíveis durante armazenamento, processamento e transmissão.

13.7 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 em mídias físicas sejam criptografados;
- ✓ Backups sejam testados no mínimo a cada 2 meses ou imediatamente após mudanças no ambiente.

13.8 Redundância dos recursos de processamento de informações

Os recursos de processamento de informação da **Elea Data Centers** são estruturados para garantir redundância e assegurar o nível de disponibilidade necessário. Além da disponibilidade, são adotadas medidas que preservam a integridade e a confidencialidade das informações nos recursos redundantes. Dessa forma, a

empresa assegura que seus sistemas e dados permaneçam acessíveis, protegidos e confiáveis.

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

O acesso aos ativos que impactam o ambiente de produção da **Elea Data Centers** é registrado e monitorado. A Elea utiliza soluções em nuvem no modelo SaaS (Software as a Service), e conta com ferramentas que permitem a visualização e auditoria dos eventos gerados, garantindo rastreabilidade, segurança e controle efetivo das atividades.

13.10 Restrição de acesso à informação

A documentação dos sistemas é devidamente protegida contra acessos não autorizados, sendo armazenada em locais apropriados e com controles que restrinjam o acesso apenas a pessoas autorizadas. Além disso, políticas e procedimentos internos reforçam essa diretriz, assegurando a confidencialidade, integridade e disponibilidade das informações documentadas.

13.11 Atividades de monitoramento

A **Elea Data Centers** adota métodos estruturados de monitoramento dos ativos, utilizando preferencialmente ferramentas automáticas e, quando necessário, mecanismos manuais, a fim de mitigar riscos e garantir a disponibilidade contínua dos serviços. Esses métodos são configurados para coletar informações relevantes, gerar evidências para a gestão de incidentes e apoiar a tomada de decisões.

13.12 Sincronização de Relógios

A **Elea Data Centers** estabelece que aplicativos, servidores e recursos tecnológicos tenham seus relógios sincronizados com o Active Directory (AD), garantindo o correto

funcionamento das aplicações, a consistência dos registros de eventos e a efetividade em eventuais investigações de segurança. Quando a sincronização com o AD não for viável, a área de TI poderá utilizar outros canais seguros para assegurar a precisão do tempo.

13.13 Softwares ilegais e direito autoral

A **Elea Data Centers** adota rigorosamente o respeito aos direitos autorais de softwares e demais materiais protegidos por propriedade intelectual, não permitindo o uso de softwares não licenciados ou ilegais. É estritamente proibida a instalação de qualquer software sem a devida licença. Para qualquer necessidade de instalação – ainda que se trate de programas que demandem apenas cópia e execução – é obrigatório solicitar a intervenção do departamento de TI.

Além disso, a Elea Data Centers não realiza cópia integral ou parcial de livros, artigos, relatórios ou quaisquer documentos sem a devida observância da legislação de direitos autorais, sendo obrigatória a citação das referências cabíveis quando aplicável.

13.14 Segurança de Redes

O acesso aos componentes da infraestrutura de produção, bem como a quaisquer outras soluções sob gestão da área de infraestrutura cloud, deve ser realizado exclusivamente por meio de mecanismos de autenticação com credenciais individuais e senhas fortes, garantindo rastreabilidade e responsabilidade do acesso. Nos casos de conexões via rede sem fio (wireless), é aconselhado a utilização de redes confiáveis, devendo evitar redes públicas.

13.15 Segregação de Redes

Os ambientes da **Elea Data Centers** são segregados por meio de tecnologia de rede VLAN (Rede de Área Local Virtual), sempre que aplicável, possibilitando a

segmentação de uma única rede comutada de forma a atender aos requisitos funcionais e de segurança de seus sistemas. As informações e aplicações utilizadas pela **Elea Data Centers** estão hospedadas em servidores na nuvem, devidamente protegidos por Firewall em software, garantindo a cobertura dos equipamentos utilizados tanto internamente, nos escritórios, quanto externamente.

Não é permitido o acesso à rede principal, seja cabeada ou wireless, por visitantes. Caso haja necessidade de conexão, será disponibilizada exclusivamente a rede destinada a visitantes, configurada para acesso restrito. A gestão de acessos às redes tem como objetivo assegurar controles adequados para criação, manutenção e revogação de acessos e permissões ao ambiente computacional da **Elea Data Centers**, observando as seguintes diretrizes:

- ✓ Somente a área de Tecnologia da Informação está autorizada a criar, alterar ou revogar acessos e/ou permissões dos sistemas e ferramentas corporativas em produção;
- ✓ Os comunicados de admissão, afastamento, férias, movimentação ou desligamento de profissionais, estagiários ou menores aprendizes devem ser formalmente encaminhados à área de Tecnologia da Informação pela área de Recursos Humanos, por meio de e-mail, garantindo a rastreabilidade e a conformidade dos processos de gestão de identidades e acessos.

13.16 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 pela empresa, que são:

- ✓ Diretórios de Repositórios (para backup e recuperação de dados em canais locais);
- ✓ Ambiente disponibilizados para compartilhamento de documentos;

- ✓ Microsoft OneDrive exclusivamente com usuário corporativo Elea Data Centers;
- ✓ E-mail institucional.

13.17 Varredura de Redes wi-fi

Para garantir o gerenciamento centralizado e seguro das redes, a **Elea Data Centers** utiliza controladora de redes wi-fi, que permite monitorar e configurar, garantindo que apenas redes autorizadas sejam utilizadas pelos colaboradores e sistemas da empresa, classificando-as como “Rede Corporativa/Conhecida” ou “Rede Desconhecida”

13.18 Filtragem Web

A **Elea Data Centers** possui uma solução de filtragem da web alinhada com suas normas e controles de segurança da informação, 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.

13.19 Norma para o uso de Controles Criptográficos

A **Elea Data Centers** estabelece e mantem documentações que garantam a confidencialidade, integridade e disponibilidade das informações, por meio da ativação de recursos de segurança e da configuração de canais seguros de comunicação. Os

documentos definem regras sobre o uso efetivo e adequado de controles criptográficos, utilizando preferencialmente a criptografia nativa dos softwares, para a proteção das informações.

Para assegurar a integridade e a recuperabilidade dos dados, é proibida a implantação de controles criptográficos não homologados pelo departamento de TI, garantindo que todas as medidas de proteção estejam alinhadas às diretrizes internas e aos padrões de segurança da **Elea Data Centers**.

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

13.19.1 Criptografia e senhas

Backup: O acesso aos backups não depende de arquivo de chave criptográfica; a proteção é realizada por meio de senha pessoal configurável pelo usuário no aplicativo. Para a restauração de backups, é necessário possuir a chave criptográfica correspondente ou credenciais de usuário autorizadas (ex.: EAD, SharePoint).

Sistemas Web: A criptografia utiliza arquivos de chave simétrica (públicos) transmitidos pela web. A validade das chaves é definida pela entidade que as emite, e os dados trafegados são protegidos por SSL em conexões HTTPS, garantindo confidencialidade e integridade.

E-mail: O e-mail utiliza a criptografia nativa do sistema. O arquivo de chave é gerado e transmitido automaticamente durante a configuração do e-mail no computador.

Sistema Operacional: O acesso é protegido por senha pessoal e intransferível, exigida no momento da inicialização do computador. Além disso, os dados do equipamento são protegidos por criptografia de disco (ex.: BitLocker), gerenciada pelo Microsoft Endpoint Manager, garantindo controle total sobre os dados criptografados. O descumprimento desta regra sujeita o usuário a sanções disciplinares.

13.20 Gestão de mudanças

A **Elea Data Centers** implementou o procedimento de Gestão de Mudanças para registrar, classificar, avaliar e aprovar as requisições de alterações nos sistemas e ambientes de TI.

Sempre que houver necessidade de mudanças nos ambientes, não é permitido utilizar dados de produção em ambientes de homologação ou testes sem o devido tratamento das informações e aprovação do responsável pelos dados.

A segregação dos ambientes de desenvolvimento, teste e produção é mandatória, garantindo que alterações acidentais ou acessos não autorizados aos sistemas e dados de negócio sejam minimizados, preservando a integridade, segurança e confiabilidade das informações da **Elea Data Centers**.

13.21 Análise Crítica de Conformidade Técnica

A **Elea Data Centers** realiza verificação e análise crítica de conformidade técnica de seus sistemas e ativos de informação. Sempre que aplicável e viável, considerando os riscos identificados, são conduzidos testes de invasão e avaliações de vulnerabilidades para identificar potenciais ameaças e reforçar a segurança.

Os processos de controle de mudanças em sistemas seguem procedimentos específicos, garantindo que alterações em plataformas operacionais, aplicação de patches e demais recursos relevantes sejam cuidadosamente analisados. Esse rigor visa prevenir instabilidades e assegurar a continuidade, integridade e confiabilidade das operações da **Elea Data Centers**.

13.22 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;
- ✓ Documentação da Instalação e Configuração, quando pertinentes;

- ✓ Senhas de administrador;
- ✓ Instalação mínima privilegiando utilização de recurso computacional;
- ✓ Desativação de Serviços Não Utilizados, quando pertinente;
- ✓ Instalação de Correções (Patches);
- ✓ Prevenção de abuso de recursos;
- ✓ Processos de validação e homologação;
- ✓ Transferência de recursos e conhecimento;

Para softwares adquiridos de terceiros e utilizados em sistemas operacionais consideramos realização de análise crítica pontual dos fornecedores.

14 Exceções

Exceções a esta política serão tratadas nos procedimentos específicos sobre cada um dos tópicos abordados.

15 Violações e sanções

15.1 Violações

São consideradas violações à política, normas ou procedimentos de segurança da informação da **Elea Data Centers** as seguintes situações, sem que esta lista seja exaustiva:

1. **Exposição a riscos:** quaisquer ações ou situações que possam colocar a **Elea Data Centers** ou seus clientes em risco de perdas financeiras, de reputação ou de ativos de informação, seja de forma direta, indireta, potencial ou real;
2. **Uso indevido de informações:** utilização ou divulgação não autorizada de dados corporativos, informações confidenciais, segredos comerciais ou qualquer outra informação sem a permissão expressa da Alta Direção;
3. **Atividades ilícitas:** uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos para fins ilícitos, incluindo violação

de leis, regulamentos internos ou externos, princípios éticos ou exigências de órgãos reguladores;

4. **Descumprimento de políticas**: não observância de qualquer item estabelecido nas documentações da **Elea Data Centers**;
5. **Falha na comunicação de incidentes:** não reportar imediatamente aos canais disponibilizados nesta política e/ou Alta direção e/ou DPO (Mais informações na Política de Privacidade) quaisquer descumprimentos desta política, normas ou procedimentos da companhia que tenham sido presenciados ou tomados conhecimento por colaboradores, estagiários, jovens aprendizes ou prestadores de serviços.

15.2 Sanções

A violação às políticas, normas ou procedimentos do SGI, bem como a não aderência à Política de Segurança da Informação, à Política de Privacidade ou ao Manual de Ética e Conduta da **Elea Data Centers**, poderá resultar em medidas disciplinares que incluem, mas não se limitam a: advertência formal, suspensão, rescisão do contrato de trabalho, aplicação de outras ações disciplinares e/ou abertura de processo civil ou criminal.

Além disso, poderão ser aplicadas sanções definidas pela Alta DIreção, sempre em conformidade com a legislação vigente, bem como as penalidades previstas na Consolidação das Leis do Trabalho (CLT).

16 Anexos

N/A

17 Registros

Lista de distribuição					
Acesso público					
Distribuição	**Armazenamento**	**Preservação**	**Recuperação**	**Retenção**	**Descarte**
Eletrônica	ECM (Enterprise Content Management ou Gerenciamento de Conteúdo Empresarial)	Backup	Data e versionamento	5 anos	Registro permanente no EAD (sistema de Arquivamento/Armazenamento de Documentos da empresa)

18 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	Atualização na disposição das informações no documento, além da classificação da informação.

			Humanos e Alta direção.	
25/08/2025	6.1	Laís Gedraits	SGI e Alta Direção	Atualização do documento, com a inclusão do canal de comunicação EHS, e novas leis como a ANPD e CLT.