ÉLIN DUXUS - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Apresentação

A Política de Segurança da Informação (PSI) visa proporcionar o entendimento de procedimentos e processos formais a fim de mitigar fragilidades no controles de sistemas e e dados acessados ou produzidos pela empresa e está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 - Sistemas de gestão da segurança da informação - Requisitos e ABNT NBR ISO/IEC 27002:2013 - Código de Prática para controles de segurança da informação e outras recomendações de boas práticas pertinentes.

Objetiva também atender aos requisitos da Lei Geral de Proteção a Dados - LGDP, não se limitando ou conflitando ao nela exposto.

Dessa forma os principais objetivos para proposição desta PSI é as garantias dos seguintes princípios:

- **Confidencialidade** – Garantia de que o acesso à informação seja obtido, apenas, por pessoas autorizadas.
- **Integridade** – Garantia de que a informação não seja adulterada falsificada ou furtada;
- **Disponibilidade** – Garantia de que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

Abrangência

Sua natureza é de ordem pública, de conhecimentos de todos os clientes, colaboradores e fornecedores que de alguma forma participam dos processos internos da empresa, devendo zelar, dentro de sua esfera de atuação, pela correta aplicação das normas aqui apresentadas na sua integralidade e permanece obrigatório por todo o tempo de duração contratual, podendo se estender por períodos posteriores em casos específicos, não sendo permitido a ninguém alegar seu desconhecimento.

Deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação. A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Está PSI deverá ser constantemente revisada em função de todos os aspectos legais vigentes e informações adicionais relevantes, sejam oriundas de práticas e ou procedimentos, novas ameaças ou tecnologias, eventos não considerados, etc. e deve obrigatoriamente refletir os requisitos do negócio e das garantias que norteiam este documento.

Normativos e Documentação Correlata à PSI

Cada um dos tópicos aplicáveis, será composto de definição do escopo, definições das normas e boas práticas, definição de procedimentos e dos seus respectivos controles da seguinte forma:

1. **Escopo**: define a apresentação e diretrizes dos tópicos desta Política.
2. **Normas e boas práticas**: especifica as boas práticas para a correta aplicação do escopo
3. **Procedimentos e Controles**: Define procedimentos para efetivação das práticas e controles com parâmetros aceitáveis para a manutenção do escopo

Pela natureza pública do presente documento, os ítens 2 e 3 são extensões desta mas de alcance restrito para as áreas afins com o intuito de balizar a gestão dos procedimentos em TI.

Conceitos e Definições

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

Agente Responsável: colaborador incumbido de chefiar e gerenciar a Equipe de Tratamento de Incidentes em Segurança da Informação;

Ameaça: conjunto de fatores externos ou causa potencial de um incidente de segurança da informação indesejado, que pode resultar em dano para um sistema ou organização;

Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Comitê Gestor de Segurança da Informação: grupo permanente de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações, que monitora, instaura regras e delibera sobre os interesses, dentre outros assuntos

Controle, Proteção ou Contramedida: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Custodiante do Ativo de Informação: responsável formal de proteger um ou mais ativos de informação, aplicando os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações.

Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

Tratamento de Incidentes em Segurança da Informação: Ato de receber, analisar e responder a notificações e atividades relacionadas a incidente de segurança em computadores;

Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso as ameaças se concretizem, que busca a oferta de uma estrutura que desenvolva a resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

Gestor da Informação: qualquer colaborador ou unidade que, no exercício de suas competências, é responsável pela produção de informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues à Élin Duxus;

Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da Élin Duxus;

Incidente de Segurança: ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação, (nos termos da Norma ISO/IEC TR nº 18044:2004 - verificar se aplicável);

Período de Retenção: período em que o backup estará disponível para retorno no tempo ou recuperação de arquivos em determinado ponto da *timeline*.

Plano de Continuidade de Negócio: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a Élin Duxus mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

Plano de Recuperação de Negócio: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a Élin Duxus operacionalize o retorno das atividades críticas à normalidade;

Plano de Tratamento dos Riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

Programa de Gestão da Continuidade de Negócio: processo contínuo de gestão e governança suportado pela alta direção que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial e manter estratégias e planos de recuperação, e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;

Recurso: é um meio de qualquer natureza (humano, físico, tecnológico, financeiro, de imagem de mercado, de credibilidade, entre outros) que permite alcançar aquilo a que se propõe;

Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

Retenção: backups de períodos (anual/mensal) já consolidados e que não estarão mais no ambiente da aplicação;

Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

RPO (Recovery Point Objective): limita o período de volta no tempo e definem a quantidade máxima permitida de dados perdidos de uma ocorrência de falha para o último backup válido.

RTO (Recovery Time Objective): está relacionado ao tempo de inatividade e representam a quantidade de tempo que leva para se recuperar de um incidente até que as operações estejam disponíveis para os usuários.

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Tratamento da Informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

Trilhas de Auditoria: arquivos de Logs do sistema, que contêm as gravações das ações realizadas no sistema, de modo a identificar quem ou o que causou algo;

Usuário Externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente à Élin Duxus;

Usuário Interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente à Élin Duxus;

Usuários: usuários internos e externos; colaboradores, terceirizados, consultores, auditores e estagiários/ bolsistas que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação.

Organização da Segurança da Informação

Organização Interna

A estrutura organizacional para gestão dos requisitos da Segurança da Informação é formado pelos grupos abaixo:

- Comitê Gestor de Segurança da Informação
- Gestores de Pessoas
- Colaboradores
- Infraestrutura

Das Responsabilidades

Comitê Gestor de Segurança da Informação

Cabe ao Comitê Gestor de Segurança da Informação:

- Propor melhorias, alterações e ajustes da PSI;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificação da informação e nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;
- Aprovar a Política de Segurança da Informação e suas atualizações

O Comitê de Gestão de Segurança da Informação deverá ser composto por:

- Diretoria
- Líderes das áreas correlatas
- Assessoria Jurídica, quando aplicável

Gestores de Pessoas e/ou Processos

Em relação à segurança da Informação, cabe aos gestores de pessoas e/ou processos:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso
- Elaborar, com o apoio da Infraestrutura, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade
- Tomar as decisões administrativas referentes aos descumprimentos da PSI

Colaboradores

Será de inteira responsabilidade de funcionários, terceirizados e demais colaboradores:

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

Infraestrutura

Cabe a Infraestrutura:

- Definir as regras para instalação de software e hardware;
- Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- Propor as metodologias e processos referentes à segurança da informação, avaliação de risco, análise de vulnerabilidades, etc.;
- Analisar criticamente incidentes de segurança em conjunto com o Comitê Gestor de Segurança da Informação;
- Manter comunicação efetiva com o Comitê Gestor de Segurança da Informação sobre possíveis ameaças e novas medidas de segurança;
- Buscar alinhamento com as diretrizes da organização.

Classificação da Informação

É de responsabilidade do Líder de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os conceitos abaixo:

- **Informação Pública:** É toda informação que pode ser acessada por usuários da organização, clientes , fornecedores, prestadores de serviços e público em geral.
- **Informação Interna:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- **Informação Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
- **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

Segurança das Operações e Comunicações

Responsabilidades e Procedimentos

Todos os processos/procedimentos para o correto funcionamento de todos os sistemas, bem como o gerenciamento de recursos é de responsabilidade da Infraestrutura.

É responsabilidade dessa também:

- Prover toda a documentação necessária para instalação, operação e recuperação dos sistemas de uso dos colaboradores e clientes.
- Processamento e tratamento da informação, tanto automática como manual
- Monitorar a correta utilização dos recursos e sugerir correções quando necessário

Proteção contra código malicioso

Manter soluções de proteção contra problemas de segurança lógica (vírus, acesso não autorizado, invasões, etc.), cabendo a Infraestrutura a definição de tais soluções de proteção, considerando a criticidade dos ativos de informação envolvidos e que estejam sob sua responsabilidade.

Caberá à mesma ainda a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalações e recuperação de softwares, sistemas operacionais, SGDBs, de forma a garantir que estes ambientes lógicos não tragam vulnerabilidades que comprometam a segurança da informação, cabendo ao Comitê de Segurança da Informação a normatização.

Segurança das Operações

A documentação pertinente do serviço e operação deve constar:

- Critérios de segurança adotados;
- A instalação e configuração
- Processamento e tratamento da informação, tanto automática como manual
- Procedimentos de cópia (backup)
- Requisitos de agendamento de operação, incluindo interdependências com outros sistemas
- Instruções de tratamento de erros ou outras condições excepcionais, que possom ocorrer
- Contatos de suporte externo para caso de eventos operacionais inesperados
- Procedimentos para reinicio e recuperação em caso de falha do sistema
- Procedimentos de monitoramento

Cópias de segurança

Todo o processo e mapas de backup, bem como os períodos de retenção deverão ser documentados e auditados quanto:

1. **Eficiência**: backups ocorrem de forma automática, sejam diários, incrementais e sincronização com pouca ou nenhum intervenção humana
2. **Disponibilidade**: backups disponíveis sempre que necessário, com tempos de RTO e RPO definidos em documentação
3. **Segurança**: todos os backups devem estar criptografados e protegidos por senha, independente da classificação da informação.

Segurança das Comunicações

Os serviços e servidores, tais como os de páginas de Internet, correio eletrônico, sistemas administrativos, serão configurados para usar tecnologias de autenticação e criptografia visando a garantir a integridade, o sigilo e a autenticidade das informações.

Providenciar para que os ambientes lógicos, tenham o seu acesso restrito por senhas seguras ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pelo Comitê Gestor de Segurança da Informação.

A Infraestrutura deve assegurar que todos os sistemas de informação, sejam aderentes as diretrizes a seguir:

- Segregação de ambientes lógicos de maneira que o ambiente de produção fique apartado dos demais
- Os ambientes de produção somente poderão ser acessados por usuários internos responsáveis pela implantação dos sistemas de informação (Infraestrutura)
- O acesso às bases de dados dos ambientes de produção será feito, sempre que possível, por meio dos sistemas de informação, ou, não sendo possível, o acesso deverá ser feito por um membro da equipe responsável pela base de dados com autorização de um usuário interno com nível gerencial da área solicitante.
- O acesso direto deverá ser registrado em meio que permita a identificação do que foi modificado e quem foi responsável pela modificação;
- Os sistemas de informação que forem transferidos para o ambiente de produção deverão ter seu código-fonte original mantido por um sistema de gerenciamento de repositórios de código-fonte interno;
- O código-fonte dos sistemas de informação deverão ser gerenciados por ferramenta específica de controle de versão. O acesso à ferramenta deverá ser restrito através de perfis de acesso específicos e registrados em trilhas de auditoria. O controle de versão deve permitir a identificação do responsável pela inclusão/ exclusão/alteração do código-fonte, assim como a recuperação de versões recentes;
- O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não deve ser utilizado para testes. Os testes devem ser feitos em ambiente apropriado e gerenciado;
- A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução

Uso do E-mail

Os usuários internos terão uma conta de correio eletrônico no serviço de correio eletrônico da Élin Duxus, que terá uma única titularidade, determinando a responsabilidade sobre sua utilização.

O e-mail não deverá ser usado para a prática de atos ilícitos proibidos pela lei ou pela presente diretriz ou normas complementares que venham a ser editadas – lesivos aos direitos e interesses da Élin Duxus ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os ativos de informação, bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

É proibido o envio de arquivos ou informações sigilosas/senhas que possam comprometer a segurança da informação, tanto na origem quanto no destino.

Arquivos com informações sigilosas devem estar zipados/criptografados e protegidos por senha. Vide alternativas para trocas de arquivos. A senha em questão não deve ser informada por e-mail. Utilizar outro meio, como por exemplo telefone, mensageiro.

Acesso Remoto

O acesso aos sistemas interno da empresa será somente através de VPN.

- Para uso dos sistemas internos com nomes de domínios não públicos, a conexão VPN proverá o DNS principal, ou seja, todas as requisições de nomes solicitadas enquanto o usuário estiver conectado na Élin Duxus serão resolvidas internamente.
- Ficam vedados o uso de quaisquer ferramentas de terceiros, sejam sistemas de compartilhamentos de arquivos (Google drive, Idrive, Dropbox, Icloud, etc), P2P, FTP, etc ou sistemas de comunicação de videoconferência, messenger's, sistemas de telefonia Voip, etc para desempenho das funções em local remoto. Para tal finalidade usar os disponíveis pela empresa, conforme documentação referente à Home Office.

Caso o local remoto disponha de roteadores Wi-Fi, o colaborador deverá atentar-se para uso indevido da rede devido à senhas fracas e ou compartilhadas. Recomenda-se que:

- A senha do Wi-Fi seja alterada com certa frequência
- Não use/ative compartilhamento de arquivos

Sistemas Internos

Todos os sistemas internos da Élin Duxus devem:

- Ser controlado por senhas de acessos, conforme as diretrizes especificadas no tópico Senhas (abaixo)
- Segregados por distribuição lógica de rede onde for aplicável
- O acesso é provido de acordo com os níveis de classificação estabelecidos no tópico Gestão de Ativos - Classificação da Informação e posição hierárquica/funcional do colaborador, definido pelos Gestores de Pessoas.

Sistemas Clientes

Todos os sistemas de acesso dos clientes hospedados na Élin Duxus devem:

- Ser controlado por senhas de acessos, conforme as diretrizes especificadas no tópico Senhas (abaixo)
- Por se tratar de acesso por meio da internet, os sistemas devem estar providos de Firewall como linha de frente, com ferramentas para detecção de ataques do tipo DDOS, *brute force* entre outros, bem como limitação de IPs que podem acessar os sistemas. Os IPs em questão devem ser comunicados à Élin Duxus para configuração do *firewall* e *proxies*
- No caso dos colaboradores das instituições clientes que trabalham em esquema de Home Office, como se trata de conexão com IPs dinâmicos, o cliente em questão deverá providenciar conexão VPN para o colaborador e usar ferramentas apropriadas para desvio das conexões aos sistemas através desse meio tendo como IP de acesso o proveniente da instituição e não do colaborador.

Senhas

A senha é um recurso pessoal e intransferível que protege a identidade do colaborador. Para todos os efeitos, fica desde já esclarecido que o uso indevido da senha de terceiros é tipificado no Código Penal Brasileiro no art 307 - Falsa Identidade.

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

- A senha é de total responsabilidade do usuário, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente comunicada à Infraestrutura no caso de suspeita de sua divulgação;
- A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderá ser fornecida por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
- É proibido o compartilhamento de login para funções de administração de sistemas, acessos à sistemas de gerenciamentos e controles, bem como para acessos à sistemas internos e administrativos da Élin Duxus;
- As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
- A senha deverá ser alterada a cada 6 meses, seguindo os preceitos acima.

O uso de aplicativo para gerenciamento das senhas de uma equipe ou colaborador pode ser adotada, desde que:

- A senha de acesso desse aplicativo siga todos os preceitos de segurança constantes nesse documento.
- Qualquer problema como acessos indevidos ao aplicativo, vazamento da senha, ou qualquer outra ação que viole a integridade da segurança dos sistema devem ser imediatamente comunicados à Infraestrutura.

Gestão de Incidentes de Segurança da Informação

Fica designado a Infraestrutura a responsabilidade para Gestão de Incidentes de Segurança da Informação, efetivando as seguintes diretrizes:

- Levantar riscos e pontos de falhas, fragilidades de segurança da informação
- Documentar processos para respostas de incidentes aos riscos levantados
- Implementar ferramentas para monitoramento, detecção, análise e notificação de incidentes e eventos
- Registrar as atividades de resolução do incidente reportado, incluindo aquelas relativa a escalação, recuperação controlada e comunicação às pessoas ou partes relevantes, internas e externas

Continuidade de Negócio

A continuidade de negócio deve ser implementada baseada em níveis de desastres estabelecidos quanto ao impacto do mesmo sobre a continuidade em si, bem como a segurança da informação, mantendo processos, procedimentos e controles para assegura o nível requerido de continuidade durante uma situação adversa.

Deve seguir os seguintes preceitos:

- A Continuidade de Negócio está implementada para mitigar e responder a um evento de interrupção
- Os recursos humanos responsáveis pela resposta ao incidente seja providos de autoridades e competência para gerenciarem um incidente e garantir a segurança da informação

Os ambientes de contingência devem ser monitorados e testados quanto a sua:

- Disponibilidade
- Segurança
- Integridade
- Resposta ao incidente, conforme documentação

A continuidade de negócios sob a ótica de gestão de empresa não é objetivo desta política, mas deve ser composta de:

- **Politica de Continuidade de Negócio**: define diretrizes para elaboração dos planos de continuidade de negócio e recuperação de negócio.
- **Plano de Continuidade de Negócio**: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a Élin Duxus mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;
- **Plano de Recuperação de Negócio**: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a Élin Duxus operacionalize o retorno das atividades críticas à normalidade;

Referências

A presente PSI segue princípios de boas prática e legislação pertinentes à saber:

- LGPD
- Série ISO 27000