Política de Segurança da Informação

Introdução

A Política de Segurança da Informação da Coimfor estabelece os princípios gerais que devem ser aplicados pela COIMFOR por si geridos no âmbito do SGSI (Sistema de Gestão de Segurança da Informação) seguindo a NP ISO/IEC 27001:2013, a legislação e regulamentação aplicáveis, específicas em matéria de segurança da informação.

A Gerência ao estabelecer o SGSI assume a presente política, os compromissos nela definidos, a integração dos requisitos do SGSI nos processos da organização e assegura que os recursos necessários à sua implementação estão disponíveis. Tem a responsabilidade para com as partes interessadas de agir de forma adequada no que respeita à gestão da segurança da informação, bem como de controlar e avaliar a implementação do SGSI.

Índice

ANEXO:

_Lista de documentação: Procedimentos

A Coimfor compromete-se a:

- Cumprir os requisitos legais e outras normas nacionais e internacionais relevantes em matéria de segurança da informação;
- Garantir a confidencialidade, integridade e disponibilidade da informação nos seus processos;
- Assegurar uma comunicação efetiva das políticas e procedimentos de segurança da informação;
- Implementar um processo contínuo de sensibilização e formação da segurança da informação;
- Demonstrar ser uma organização segura em matéria de segurança da informação.

Âmbito

A Política de Segurança da Informação da COIMFOR destina-se a todas as partes interessadas.

Todas as partes interessadas têm de conhecer e agir em conformidade com a Política de Segurança da Informação da COIMFOR e com os demais documentos relacionados com a Segurança da Informação, conforme aplicável e adequado.

Todas as partes interessadas que estão abrangidas pelo SGSI e que deliberadamente violem esta ou outras políticas ficam sujeitas a sanções e outras ações, que podem ir até à cessação do contrato e/ou à participação às autoridades policiais ou judiciais das situações que indiciem a prática de crime.

Valor da Informação

A informação pode adotar diversas formas (estar impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou meios eletrónicos, entre outras), devendo ser adequadamente protegida, independentemente do seu meio, utilização ou suporte. A segurança da informação deverá estar ajustada face à sua importância e valor.

O acesso à informação é vital no funcionamento da COIMFOR dependendo da disponibilidade dos sistemas e infraestruturas de informação. A segurança no tratamento e transmissão da informação é assim fundamental para a eficiência do processo de produção e distribuição de software.

Qualquer interrupção do serviço, fuga de informação para entidades não autorizadas ou modificação não autorizada de dados pode levar a uma perda de confiança e/ou violar as obrigações legais e contratuais para com cidadãos e empresas. É da responsabilidade de todas as partes interessadas contribuírem proativamente para a segurança da informação.

No entanto, tal apenas se torna possível com a identificação contínua dos riscos aos quais os ativos, nomeadamente sob responsabilidade da COIMFOR se encontram expostos, bem como pela implementação de controlos e mecanismos de segurança que visem a utilização correta e controlada dos mesmos.

Importância da Segurança da Informação

A informação gerida pela **COIMFOR**, os seus processos de suporte, sistemas, aplicações e redes são ativos valiosos para a empresa.

A garantia de confidencialidade, integridade e/ou disponibilidade da informação assegura a credibilidade dos serviços prestados pela COIMFOR.

A segurança da informação deverá, portanto, ser aplicada em todas as fases do ciclo de vida das atividades prosseguidas pela COIMFOR. O controlo de segurança da informação das operações de inserção / recolha, processamento, armazenamento, transferência, relacionamento, pesquisa e destruição da informação é tão ou mais importante do que a funcionalidade de um sistema de informação. Deve, assim, ser assegurada a manutenção de forma permanente e equilibrada de um nível de qualidade e segurança elevados, prevenindo a materialização de riscos inerentes para mitigar/ limitar os potenciais danos provocados pela exploração de vulnerabilidades e incidentes de segurança da informação.

As ameaças à segurança da informação estão em constante evolução, o que implica a adaptação contínua de medidas de segurança da informação de modo a acompanhar as alterações tecnológicas e legislativas ou regulamentares. As medidas de segurança da informação devem ser técnica e economicamente viáveis e não devem limitar a produtividade e eficiência da COIMFOR.

Linhas orientadoras para a Gestão da Segurança da Informação

- **Gestão de pessoas:** a Política de Segurança da Informação é aplicável a todos os utilizadores da COIMFOR e deve ser aplicada de forma transversal em todos as unidades orgânicas, devendo ser estabelecidas responsabilidades específicas em determinadas funções;

- **Gestão do risco:** todos os sistemas (existentes ou planeados) devem ter um nível de segurança da informação adequado face ao risco a assumir pela COIMFOR;

- **Definição de responsabilidades:** a responsabilidade pela qualidade, acessos, utilização e salvaguarda da informação contida nos sistemas é da COIMFOR. Cabe à COIMFOR definir as normas e procedimentos que implementem os níveis de segurança da informação definidos pelas entidades proprietárias da informação e vigiar a sua efetividade;

- **Políticas de segurança da informação:** devem existir políticas de segurança da informação detalhadas aplicáveis a todos os sistemas de informação, independentemente do seu ambiente;

- **Procedimentos de segurança da informação:** devem existir procedimentos o mais detalhados possível que definam "o quê" e "como" atingir o nível de segurança da informação pretendido, bem como a definição do nível de envolvimento humano na manutenção dos sistemas de informação;

- **Rastreabilidade dos sistemas de informação:** as operações nos sistemas de informação devem estar devidamente documentadas, assegurando que a qualquer momento é possível aferir "quem" e "quando" fez "o quê";

- **Monitorização de controlos:** a implementação de controlos que enderecem os riscos aos quais o negócio se encontra exposto só é eficaz se existir uma adequada monitorização dos controlos, de forma a avaliar se os mesmos se encontram ajustados face aos objetivos definidos. Igualmente, devem estar definidas ações de resposta atempada quando se verifique a não operacionalidade dos controlos.

Modelo do Sistema de Gestão de Segurança da Informação

O modelo do SGSI da COIMFOR assenta em três vetores:

- **Confidencialidade:** garantia que a informação está acessível apenas a utilizadores e entidades externas) devidamente autorizados para o efeito;
- **Integridade:** salvaguarda da exatidão da informação e dos métodos de processamento;
- **Disponibilidade**: garantia que utilizadores autorizados têm acesso à informação sempre que necessário.

Associados aos 3 pilares fundamentais, existem ainda outros conceitos de Segurança da Informação que importa clarificar para garantir um entendimento comum na organização:

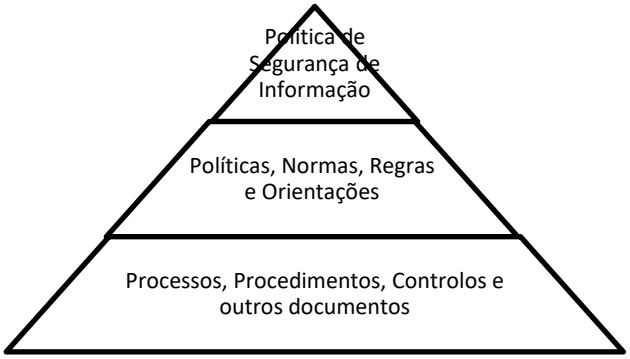
• **Privacidade** - Conceito associado à Confidencialidade. Compreende a proteção da informação, em especial dos dados pessoais dos clientes, colaboradores ou outros titulares, com o objetivo de garantir o cumprimento das normas legais aplicáveis e do direito fundamental de cada indivíduo de ter acesso e decidir quem deve ter acesso, em cada momento, aos seus dados.

• **Não Repudio** - Conceito associado à Integridade. Assegura que existe evidência que permite verificar a ocorrência de uma determinada ação ou evento e que permite identificar inequivocamente o originário de uma comunicação ou o responsável por uma operação.

• **Resiliência** - Conceito associado à Disponibilidade. Assegura que os ativos de suporte à informação (sistemas, plataformas, infraestruturas, outros ativos) têm a capacidade para resistir a um incidente e para continuar a disponibilizar a informação/serviços.

• **Retenção -** Conceito associado à Disponibilidade. Assegura que a informação só pode ser conservada pelo tempo necessário para o negócio e que é permitido por lei.

Todos os mecanismos de segurança da informação existentes na COIMFOR visam a confidencialidade, integridade e/ou disponibilidade da informação, e devem ser regulados por um corpo normativo constituído por políticas detalhadas, processos e procedimentos de segurança da informação, encontrando-se estruturado da seguinte forma:



Políticas detalhadas de Segurança da Informação

A Política de Segurança da Informação expressa as considerações da COIMFOR no que respeita à segurança da informação sobre os seguintes aspetos:

1. Aspetos elementares da Segurança da Informação: A gestão da segurança da informação e dos sistemas que a suportam é realizada garantindo, através de uma abordagem baseada na gestão de risco e na melhoria contínua, a confidencialidade, a integridade e a disponibilidade da informação. Neste sentido a **COIMFOR** compromete-se a:

a) A garantir a segurança da informação que titula, assim como de todos os recursos a ela associados, sejam eles processuais, tecnológicos ou humanos.
b) Assegurar o estabelecimento e a prossecução dos princípios descritos nesta política, bem como a sua aprovação, publicação e comunicação a todos os colaboradores e entidades externas relevantes;
c) Garantir os recursos necessários para a operacionalização dos processos e atividades de gestão da segurança da informação;
d) Assegurar a definição, implementação e revisão da estratégia de gestão de segurança da informação e garantir o correto alinhamento com as políticas e objetivos estratégicos de negócio da COIMFOR;
e) Assegurar que o SGSI atinge os resultados pretendidos;
f) Promover, de forma estruturada e sistemática, a melhoria contínua.

2. Classificação e Manuseamento da Informação: Definindo-se ativo de segurança de informação como qualquer recurso com valor para a organização, estes são classificados em função da sua sensibilidade relativamente aos seus atributos, designadamente a confidencialidade, integridade e disponibilidade, de modo a aplicar os controlos adequados para a sua salvaguarda.

3. Utilização de dispositivos móveis e de acesso remoto: São aplicadas medidas de segurança à utilização de dispositivos móveis diferenciados entre utilizadores e assistência técnica / produção da COIMFOR, para garantir a confidencialidade, integridade e a disponibilidade da informação de negócio para que possa ser acedida (de forma local ou remota) e/ou processada por estes dispositivos.

4. Uso aceitáveis de ativos: Os ativos de informação propriedade da COIMFOR são utilizados de forma a garantir a sua proteção, evitando a exposição dos mesmos a riscos de Segurança de Informação com potencial impacto de comprometerem a continuidade de negócio da COIMFOR. A COIMFOR concede aos seus colaboradores e clientes o direito de utilizar os seus próprios equipamentos, desde que sejam cumpridas as orientações internas.

5. Relação com fornecedores: Os fornecedores são avaliados de forma a garantir relações contratuais com entidades que contribuem para a obtenção de acesso a matérias e serviços adequados ao negócio da COIMFOR.

Os termos de responsabilidade elaborados pela COIMFOR, para adjudicação de contratos de fornecimentos de bens ou serviços compreendem aspetos que garantem a Segurança da Informação, estipulando responsabilidades e deveres do fornecedor.

6. Controlos de acesso físico e lógico: Estão implementados controlos de acesso físico e lógico que permitem a gestão de identidades através de processos de identificação e autenticação do utilizador e que, por sua vez, permitem a implementação de regras de restrição baseadas em critérios de segurança.

Os diferentes perfis, privilégios e níveis de acesso físicos e lógicos são definidos seguindo o Princípio do Privilégio Mínimo, ou seja, pela atribuição do nível de acesso estritamente necessário para o utilizador desempenhar as funções atribuídas e não mais.

7. Criptografia: A COIMFOR implementa mecanismos criptográficos para proteger informação lógica de acessos não autorizados.

8. Mesa e ecrã limpo: As informações consideradas sensíveis, em formato físico ou digital, são devidamente protegidas sempre que não se encontram em uso.

9. Cópias de Segurança: São efetuadas cópias de segurança, que ocorrem com uma periodicidade definida de forma a salvaguardar a informação. Os colaboradores e clientes são responsáveis pelas cópias de segurança da informação contida nos equipamentos a seu cargo. Os colaboradores comprometem-se a cumprir as políticas de segurança para salvaguardar a informação ao seu dispor.

10. Transferência de Informação: A informação é trocada em canais de comunicação aprovados seguindo os requisitos de segurança definidos consoante a sua classificação de segurança.

11. Princípios de engenharia e política de desenvolvimento de sistemas de informação seguros: São aplicados princípios de desenvolvimento de sistemas de informação seguros em todos os níveis da arquitetura de sistemas (negócio, dados, aplicações e tecnologia) balanceando a necessidade de segurança com a necessidade de acessibilidade/eficiência funcional. Os princípios são considerados durante todo o ciclo de vida dos sistemas de informação numa perspetiva evolutiva.

12. Segurança da Informação na Gestão de Projetos: A segurança da informação é endereçada na gestão de projetos através da identificação de possíveis riscos de segurança de informação associados ao projeto a implementar.

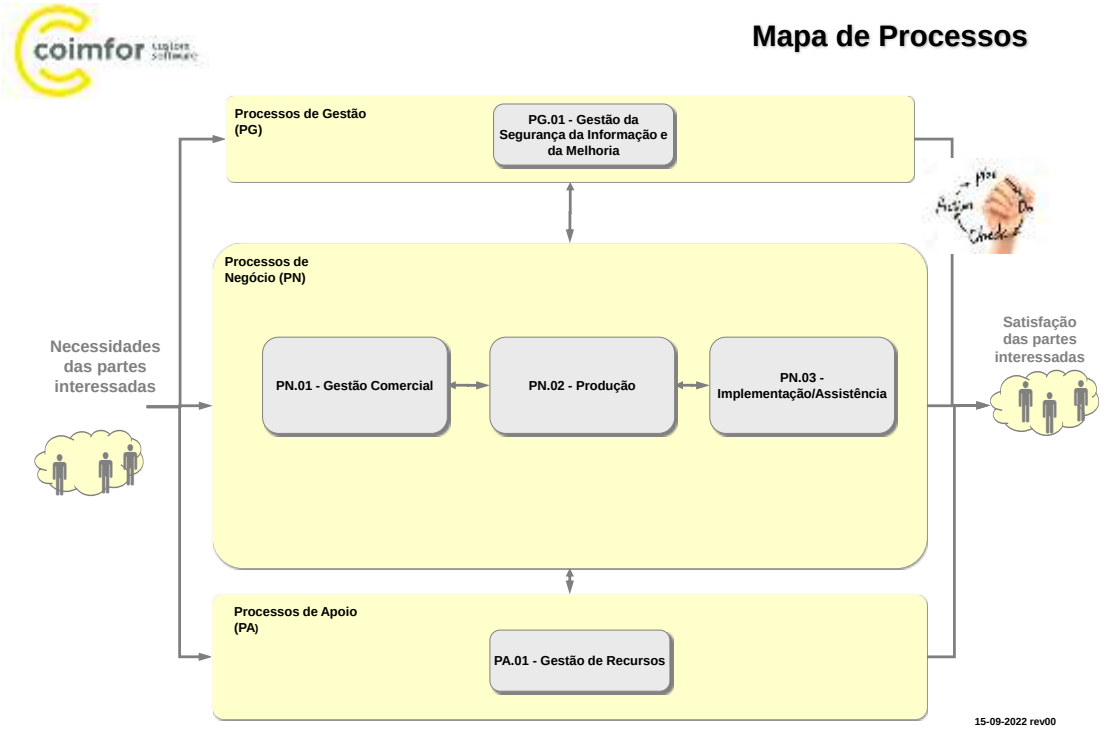
13. Gestão de Riscos e Gestão de Incidentes e Continuidade de Negócio: São identificados, analisados, quantificados/qualificados os riscos decorrentes de várias fontes de risco para os seus ativos de informação.

Os eventos que colocam em causa ou tenham potencial de colocar em causa os compromissos de Segurança de Informação são tratados como possíveis incidentes de segurança e são tratados de acordo com o processo de **Gestão de Incidentes interno.**

A continuidade da Segurança da Informação é contemplada na continuidade de negócio, de tal forma que contempla a perda de recursos de informação através da implementação de controlos preventivos e de recuperação.

14. Perfis, Responsabilidades e Autoridades do SGSI: Encontram-se definidos os papéis, responsabilidade e autoridades para fazer cumprir os comprometimentos da COIMFOR perante a Segurança da Informação.

Mapa de Processos



Lista de Procedimentos

Consultar anexo A

Organização da Segurança da Informação

A organização da segurança da informação visa estabelecer, implementar, manter e melhorar continuamente o SGSI no contexto da organização e especifica os requisitos para a avaliação e tratamento de riscos de segurança da informação à medida das necessidades da COIMFOR.

A estrutura de gestão do SGSI é constituída por:

Funções	Responsabilidades
Gerência e Responsável de Segurança da Informação (SI)	Tem a responsabilidade de controlar e avaliar a implementação do SGSI; Que participa ativamente no desenvolvimento do SGSI, em especial na Política de privacidade e protecção de informações de identificação pessoal e nos temas com implicações na proteção de dados pessoais
Resp. Qualidade	Que tem a responsabilidade de gerir o SGSI;

Equipa de Segurança da Informação	É responsável pela implementação de mecanismos de segurança da informação;
Responsáveis departamento e/ou outros colaboradores	Que atuam como facilitadores em todas as unidades orgânicas da COIMFOR
Colaboradores	• Conhecer e cumprir com as políticas, normas e procedimentos SGSI, bem como com as legislações e regulamentações. • Aplicar as regras de SGSI by Design no desenvolvimento de processos e sistemas, assim como operacionalizar, monitorizar e manter os respetivos controlos de SGSI. • Reportar à Gerência / Responsável de Segurança da Informação alterações em atividades ou em parceiros que tenham impacto no Registo de Atividades de Tratamento (RAT). • Garantir o tratamento de eventuais não conformidades do SGSI, identificadas por exemplo nas auditorias internas e externas ou pelos próprios departamentos • Efetuar a participação de eventuais incidentes de SGSI ou qualquer violação através dos canais definidos. • Estar consciente de que a violação por parte de um Colaborador COIMFOR de qualquer norma, regra ou procedimento interno enquadrável nas Políticas do SGSI da COIMFOR constitui um ilícito disciplinar, passível de sanção, consoante a gravidade da infração, podendo incorrer em responsabilidade civil e criminal do Colaborador. No caso de Colaborador de Parceiro, aplicar-se-ão, através dos Parceiros, as sanções previstas na lei ou em contrato.

Manutenção e comunicação das políticas e procedimentos de segurança da informação

As políticas e procedimentos de segurança da informação devem ser do conhecimento de todas as partes interessadas, no respetivo âmbito de aplicação, e deve assegurar-se uma comunicação efetiva das políticas e procedimentos de modo a que as partes interessadas sejam conhecedoras das obrigações individuais quanto à temática da segurança da informação.

As políticas e procedimentos de segurança da informação são regularmente revistos, garantindo que continuam a ser relevantes e adequados.

Histórico do Documento		
Data	**Nº Versão**	**Descrição**
30-11-2022	00	Emissão do documento