POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Versão	1.0
Data da Versão	19/09/2025
Responsável	Fabrício Alves Pereira
Classificação	Documento Publico
Aprovado por	Comitê de Segurança da Informação

Sumário

1. **Finalidade, escopo e usuários** 2
2. **Referências** 2
3. **Gerenciando a segurança da informação** 2
3.1. **Objetivos e medição** 2
3.2. **Requisitos de segurança da informação** 3
3.3. **Controles da segurança da informação** 3
4. **Responsabilidades** 3
5. **Suporte para a implementação do SGSI** 5
6. **Validade e gestão de documentos** 5
7. **Histórico de alterações** 5

1. Finalidade, escopo e usuários

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de Gestão da Segurança da Informação (SGSI), como definido no documento de escopo do SGSI.

Este documento, assim como toda a documentação referente ao Sistema de Gestão, é de propriedade da CPRV, divulgados e controlados pela área de tecnologia da informação, sendo proibida a reprodução indevida ou divulgação destes documentos sem consentimento prévio.

A Segurança da Informação visa a preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade. A segurança compreende, assim, a proteção das informações em relação aos diversos tipos de ameaças para: · garantir a continuidade do negócio; · minimizar o risco ao negócio; · maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Os usuários deste documento são todos os colaboradores, contratados, prestadores de serviços da CPRV, assim como as partes externas relevantes.

2. Referências

- Norma ISO/IEC 27001, em sua versão atual
- Lei nº13.709/2018 - Lei Geral de Proteção de Dados (“LGPD”).
- Manual Sistema de Gestão de Segurança da Informação - SGSI – CRPV, em sua versão atual
- Lista de Obrigações Legais - CPRV.

3. Gerenciando a segurança da informação

3.1. Objetivos e medição

- **Obter a Certificação da Norma ISO/IEC 27001:** Demonstrar o comprometimento da organização com as melhores práticas de segurança da informação, através do reconhecimento formal de um organismo certificador.
- **Qualificação da Empresa Perante o Mercado:** Fortalecer a reputação e a credibilidade da CPRV como uma empresa segura e confiável, atendendo às expectativas de clientes, parceiros e reguladores.
- **Elevar a Proteção de Acesso a Sistemas:** Implementar controles de acesso robustos como Autenticação Multifator (MFA), VPN para acesso a sistemas e revisões de privilégios, implementar criptografia de dados em repouso e em trânsito.
- **Gestão de Incidentes:** Garantir que a CPRV está preparada para responder de forma rápida e eficiente a qualquer evento de segurança. Isso inclui desde a detecção inicial até a completa recuperação, minimizando o impacto em suas operações, dados e reputação.
- **Conscientização e Treinamento sobre Segurança e Privacidade:** Promover uma cultura de segurança da informação, educando e conscientizando todos os colaboradores sobre suas responsabilidades na proteção

dos dados.

Os objetivos dos controles de segurança ou grupos de controles são definidos pela alta direção da CPRV e aprovados pelo Comitê de Segurança da Informação na Declaração de aplicabilidade.

A CPRV irá mensurar o atendimento de todos os objetivos. O responsável pela área de tecnologia da informação em conjunto com o responsável pela área de SOC, são os responsáveis por definir o método para a medição da realização dos objetivos, a medição será executada ao menos uma vez por ano e o responsável pela área de projetos que irá analisar a avaliar os resultados da medição e reportá-los para a alta direção da CPRV como materiais de entrada para a análise crítica.

O responsável pela área de Projeto é responsável por registrar os detalhes sobre os métodos de medição, periodicidades e resultados no relatório de medição.

Todos os objetivos devem ser revisados pelo menos uma vez por ano.

3.2. Requisitos de segurança da informação

Esta Política de Segurança da Informação (PSI) e todo o Sistema de Gestão da Segurança da Informação (SGSI) da CPRV devem estar em plena conformidade com todos os requisitos legais, regulatórios e obrigações contratuais aplicáveis.

A CPRV assegura que a Política de Segurança da Informação (PSI) seja amplamente comunicada e acessível a todas as partes interessadas relevantes, seus colaboradores, parceiros, clientes e prestadores de serviços, através de canais como a intranet e a publicação em seu site. O objetivo é garantir que cada indivíduo compreenda claramente sua responsabilidade em cumprir as diretrizes da política, agindo como um agente de proteção das informações da empresa, independentemente de sua localização.

O não cumprimento dos requisitos previstos neste documento acarretará violação às regras internas da CPRV, e sujeitará o usuário às medidas administrativas e legais cabíveis.

3.3. Controles da segurança da informação

Os processos para selecionar os controles (salvaguardas) estão definidos na Metodologia de avaliação e tratamento de riscos.

Os controles selecionados e seu status de implementação estão listados na Declaração de aplicabilidade.

4. Papeis e Responsabilidades

A responsabilidade pela Segurança da Informação (SI) é distribuída em níveis hierárquicos e funcionais, sendo:

4.1. Alta Administração e Comitê de Segurança da Informação (CSI)

- **Alta Administração:** É responsável por garantir que o Sistema de Gestão de Segurança da Informação (SGSI) seja estabelecido, implementado, mantido e melhorado continuamente, assegurando que os recursos necessários (financeiros e humanos) estejam disponíveis para o cumprimento desta PSI.
- **Comitê de SI:** É o órgão de governança do SGSI. Responsável pela revisão e aprovação desta Política e de seus documentos derivados, monitorando o desempenho do SGSI e tomando decisões estratégicas baseadas na análise de riscos.

4.2. Gestão de Tecnologia da Informação (TI)

A TI atua como o principal **proprietário dos ativos** e é responsável pela administração geral da infraestrutura.

- Executar a criação, alteração e bloqueio de utilizadores. Configurar tecnicamente a Autenticação Multifator (MFA) e a VPN.
- Configurar servidores e estações de trabalho eliminando funções desnecessárias que possam servir de porta para ataques.
- Aplicar atualizações de segurança em todos os sistemas e aplicações de forma tempestiva.
- Garantir que todos os notebooks e discos rígidos da CPRV tenham criptografia ativa (ex: BitLocker) e que o tráfego de rede seja cifrado (SSL/TLS).
- Executar as rotinas de cópia de segurança e, mais importante, **realizar testes de restauro** periódicos para garantir que os dados são recuperáveis.
- Manter atualizada a lista de hardware, software e licenças em uso na CPRV.
- Garantir que todos os dispositivos têm a proteção de endpoint instalada, atualizada e ativa.
- Monitorizar o "uptime" dos sistemas críticos para cumprir os objetivos de continuidade de negócio da CPRV.

4.3. Security Operations Center (SOC)

O SOC é a primeira linha de defesa da CPRV, responsável pela **Confidencialidade** e **Integridade** dos dados.

- Analisar em tempo real os eventos gerados pelo SIEM (Security Information and Event Management), distinguindo falsos positivos de ameaças reais.
- Monitorizar proativamente os alertas vindos do EDR (Endpoint Detection and Response) em todos os computadores da empresa.
- Identificar padrões anómalos, ou um volume atípico de exportação de dados.
- Executar o bloqueio imediato de contas comprometidas ou o isolamento de máquinas infectadas da rede para impedir a propagação (movimentação lateral).
- Apoiar o Comitê na descoberta de *como* o atacante entrou, para que a TI possa "fechar a porta" tecnicamente.
- Notificar o Comitê de Segurança e a TI sempre que um incidente de impacto **Médio ou Alto** for confirmado.

4.4. Network Operations Center (NOC)

O NOC é a primeira linha de suporte da CPRV, responsável pela **Disponibilidade** e Performance dos serviços.

- Verificar a saúde de *routers*, *switches*, *firewalls* e servidores, garantindo que não haja sobrecarga de CPU ou memória.
- Acompanhar se serviços críticos (E-mail, ERP, VPN) estão respondendo dentro dos tempos normais de latência.
- Prever quando a CPRV precisará de mais armazenamento ou processamento, evitando que o sistema pare por falta de recursos.
- Realizar alterações na configuração da rede seguindo o processo de **Gestão de Mudanças** para evitar paragens não planeadas.

4.5. Todos os Colaboradores

Todos os colaboradores, terceiros e contratados têm a responsabilidade individual de:

- Cumprir integralmente as diretrizes desta PSI e dos seus documentos derivados (como a Política de Teletrabalho e a Política de Uso de BYOD).
- Proteger os ativos de informação que lhes são confiados, garantindo a sua confidencialidade, integridade e uso seguro.
- Reportar imediatamente quaisquer incidentes, vulnerabilidades ou suspeitas de violação de segurança à equipe do **SOC** ou **TI**.

5. Suporte para a implementação do SGSI

A alta administração da CPRV declara que a implementação do SGSI e seu contínuo aprimoramento serão suportadas pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como atender todos os requisitos identificados.

6. Validade e gestão de documentos

Este documento passa a ser válido a partir da data de aprovação do Comitê de Segurança da Informação.

O proprietário do documento é o responsável pela área de Tecnologia da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes relacionados ao acesso não autorizado às informações
- quantidade de ativos de informações classificados com o nível de confidencialidade inadequado

Penalidades e Consequências

O não cumprimento das diretrizes desta política poderá resultar em ações disciplinares, que podem incluir advertências, ou até rescisão contratual, dependendo da gravidade da infração. Em caso de incidentes de segurança, podem ser tomadas medidas corretivas adicionais.

Treinamento e Conscientização

- **Sensibilização**: Todos os colaboradores devem ser devidamente informados e sensibilizados quanto às políticas de segurança da informação da organização, compreendendo sua importância para a proteção dos ativos e a continuidade do negócio.
- **Conscientização sobre Segurança**: A CPRV deve promover treinamentos periódicos com foco nas melhores práticas de segurança da informação, visando prevenir incidentes, reforçar comportamentos seguros e assegurar que cada colaborador conheça suas responsabilidades individuais no tratamento adequado das informações.

7. Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
19/09/2025	1.0	Fabrício Alves Pereira	Versão Inicial do documento