CORPVS
QUEM TEM ESTÁ SEGURO
DESDE 1975

CORPVS
SEGURANÇA

Quem tem, está seguro!

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Código: D-PSI-001

1. Introdução

1.1. Este documento estabelece a Política de Segurança da Informação **D-SI-001** no âmbito da CORPVS com o objetivo de estabelecer diretrizes e normas gerais para a gestão da segurança da instituição. De forma específica, visa fornecer uma orientação quanto ao uso adequado de recursos, proteção de ativos, pessoas e de informações. Objetiva definir responsabilidades, obrigações e direcionamentos para a gestão da segurança das pessoas, da segurança física e patrimonial e da segurança da informação, evitando assim impactos prejudiciais às atividades finalísticas e à Gestão da Instituição. Cria controles para a execução dos processos de negócios da CORPVS, em relação ao manuseio e proteção das informações, acessos não autorizados, sejam eles acidentais ou intencionais, garantindo a continuidade dos serviços e fortalecendo a credibilidade e imagem da Instituição.

1.2. A Política de Segurança Corporativa aqui estabelecida deve servir como um guia para todas as unidades administrativas da CORPVS implementarem e manterem a gestão dos controles de segurança nos seus ambientes de trabalho.

1.3. Dessa forma, a CORPVS estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. Propósito

2.1. A Política de Segurança da Informação será norteada pelos seguintes princípios, sem prejuízo dos princípios da CORPVS:

2.1.1. Alinhamento estratégico: deve haver um alinhamento entre as diretrizes, normas e ações de segurança da CORPVS com a sua missão institucional e seu planejamento estratégico.

2.1.2. Diversidade organizacional: a elaboração de diretrizes, normas e controles de Segurança Corporativa da CORPVS devem levar em consideração a diversidade das atividades da Instituição, respeitando a natureza e finalidade da organização.

2.1.3. Propriedade da informação: toda informação produzida ou armazenada na CORPVS é de sua propriedade e não de seus colaboradores, exceto os casos em que a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição.

2.2. Resguardar as informações da CORPVS, garantindo requisitos básicos de confidencialidade, integridade, disponibilidade, autenticidade, não repudio e conformidade;

2.3. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

2.4. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da CORPVS como resultado de falhas de segurança.

2.5. Implementar os controles necessários para cumprir os requisitos de segurança da informação necessários à proteção da privacidade e de dados pessoais tratados pela CORPVS.

2.5.1. Adotar medidas de segurança, tanto técnicas quanto administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme padrões mínimos recomendados pela Autoridade Nacional de Proteção de Dados Pessoais.

2.5.2. Apoiar o Encarregado pelo tratamento de dados pessoais na comunicação à Autoridade Nacional e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar riscos ou danos.

2.5.3. Realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável;

3. Escopo

3.1. Esta política se aplica a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes, em desenvolvimento ou que venham a ser adquiridos pela CORPVS, incluindo qualquer indivíduo ou organização que possui, possuiu ou possuirá vínculo com a CORPVS, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, consultores externos, que possuíram, possuem ou virão a possuir acesso às informações da CORPVS e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura CORPVS.

4. Diretrizes

4.1. O objetivo da gestão de Segurança da Informação da CORPVS é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e

minimizando riscos identificados e não identificados e seus eventuais impactos a instituição.

4.2. A Presidência, Diretoria Executiva e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na CORPVS. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da CORPVS.

4.3. É política da CORPVS:

4.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da CORPVS sejam atingidos através da adoção de controles contra ameaças provenientes de fontes externas e internas;

4.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes.

4.3.3. Garantir a educação e conscientização sobre as práticas adotadas pela CORPVS de segurança da informação para Empregados, terceiros contratados e, onde pertinente, clientes.

4.3.4. Atender integralmente os requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

4.3.5. Tratar integralmente todos os incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

4.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

4.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5. Papéis e Responsabilidades

5.1. Todos os colaboradores da CORPVS, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos físicos, tecnológicos e informações de que sejam usuários, dos ambientes físicos e

computacionais a que tenham acesso, independente das medidas de segurança implementadas.

5.2. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI

5.2.1. Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico, Comunicação.

5.2.2. É responsabilidade do CGSI:

5.2.2.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

5.2.2.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

5.2.2.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

5.2.2.4. Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da CORPVS.

5.3. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

5.3.1. É responsabilidade da Gerência de Segurança da Informação:

5.3.1.1. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

5.3.1.2. Apoiar o CGSI em suas deliberações;

5.3.1.3. Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSI;

5.3.1.4. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas preventivas para reduzir o risco;

5.3.1.5. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

5.3.1.6. Realizar a gestão dos incidentes de segurança da informação realizando adequadamente os registros, classificação e documentação dos mesmos.

5.4. GESTORES DA INFORMAÇÃO

5.4.1. É responsabilidade dos Gestores da Informação:

5.4.1.1. Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela CORPVS;

5.4.1.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela CORPVS;

5.4.1.3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

5.4.1.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.4.1.5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela CORPVS.

5.5. USUÁRIOS DA INFORMAÇÃO

5.5.1. É responsabilidade dos Usuários da Informação:

5.5.1.1. Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

5.5.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

5.5.1.3. Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da CORPVS;

5.5.1.4. Assinar o Termo de Uso de Sistemas de Informação da CORPVS, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.

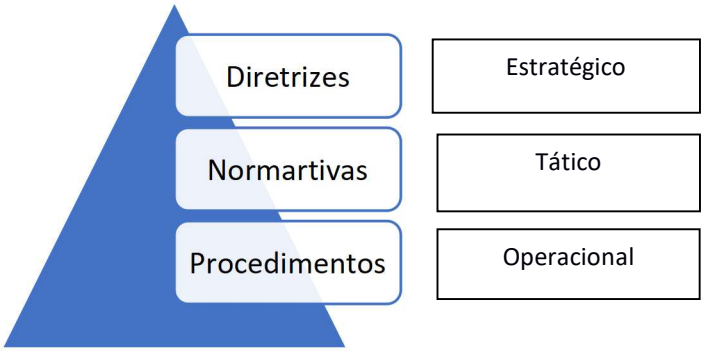
6. Estrutura da Segurança Corporativa

6.1. A estrutura normativa da Segurança da Informação da CORPVS é composta por um conjunto de documentos classificados em 03 (três) níveis hierárquicos distintos:

6.1.1. Política de Segurança da Informação: está relacionada ao nível estratégico, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação, bem como descreve o que deve ser feito.

6.1.2. Normas de Segurança da Informação: estão relacionadas ao nível tático, estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política a serem seguidos em diversas situações em que a informação é tratada, são as regras a serem adotadas.

6.1.3. Procedimentos de Segurança da Informação: estão relacionados ao nível operacional, instrumentalizam o disposto nas Normas e na Política, descrevendo os procedimentos a realizar, permitindo a aplicação direta nas atividades da CORPVS, definindo como serão implementadas as regras.



7. Planos e Normas que compõem a Política de Segurança da Informação

7.1. Os Planos e Normas de Segurança Corporativa aplicável à CORPVS estão definidas para abranger as três disciplinas da Segurança Corporativa, a saber:

7.2. Segurança da Informação

7.2.1. Norma de Gestão de Risco de TI;
7.2.2. Norma de Backup e Restauração de Segurança;
7.2.3. Norma de Implementação e Atualização de Segurança;
7.2.4. Norma de Gestão de Vulnerabilidade de TI;
7.2.5. Norma de Hardening;
7.2.6. Norma de Gestão de Identidade e Controle de Acesso;
7.2.7. Norma de Gestão de Incidentes;
7.2.8. Norma de Uso do Ambiente em Cloud;
7.2.9. Norma de Classificação da Informação;
7.2.10. Norma de Acesso Remoto;
7.2.11. Norma de Procedimento de Investigação de Análise Forense;
7.2.12. Norma de Gestão de Ativos;
7.2.13. Norma de Gestão da Continuidade do Negócio de TI;
7.2.14. Norma de Correio Eletrônico;
7.2.15. Norma de Gestão de Pessoas;
7.2.16. Norma de Internet e Mídias Sociais;
7.2.17. Plano de Recuperação de Desastre;
7.2.18. Plano de Resposta à Incidentes;
7.2.19. Plano de Gerenciamento de Crises.

8. Violações e Sanções

8.1. Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas poderão ser adotadas para averiguar a responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se ao direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, sem prejuízo de ação civil e penal, se aplicáveis.

8.2. O não cumprimento da Política de Segurança Corporativa por parte de terceiros, prestadores de serviço ou fornecedores que estejam atuando no âmbito da CORPVS, ainda que por desconhecimento, poderá acarretar sanções legais e/ou administrativas, conforme previstas no contrato de prestação de serviços celebrado entre a CORPVS e a prestadora de serviços.

8.3. O não cumprimento da Política de Segurança Corporativa por parte de estagiários, ainda que por desconhecimento, poderá acarretar sanções legais e/ou administrativas, conforme previstas no Termo de Compromisso de Estágio.

8.4. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar

que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

9. Exceções

9.1. Requerimentos de exceção do disposto neste documento normativo deverão ser submetidos à aprovação do comitê de segurança da CORPVS.

9.2. As exceções serão avaliadas pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

9.3. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da CORPVS adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações de negócios da CORPVS.

10. Documentos Complementares

10.1. Norma de Gestão de Risco de TI;
10.2. Norma de Backup e Restauração de Segurança;
10.3. Norma de Implementação e Atualização de Segurança das Estações de
10.4. Norma de Gestão de Vulnerabilidade de TI;
10.5. Norma de Hardening;
10.6. Norma de Gestão de Identidade e Controle de Acesso;
10.7. Norma de Gestão de Incidentes;
10.8. Norma de Uso do Ambiente em Cloud;
10.9. Norma de Classificação da Informação;
10.10. Norma de Acesso Remoto;
10.11. Norma de Procedimento de Investigação de Análise Forense;
10.12. Norma de Gestão de Ativos;
10.13. Norma de Gestão da Continuidade do Negócio de TI;
10.14. Norma de Correio Eletrônico;
10.15. Norma de Gestão de Pessoas;
10.16. Norma de Internet e Mídias Sociais;
10.17. Plano de Recuperação de Desastre;
10.18. Plano de Resposta à Incidentes;
10.19. Plano de Gerenciamento de Crises.

11. Revisões

11.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

VER	DATA EMISSÃO	ALTERADA A PARTIR DE	DESCRIÇÃO DA ALTERAÇÃO	TEMPO DE RETENÇÃO DO DOCUMENTO OBSOLETO
01	30/05/2022	-	Criação	-
02	30/05/2022	10/03/2023	Atualização, revisão e correção textual	1 ano
03	30/05/2022	09/10/2023	Atualização, revisão e correção textual	1 ano

12. Gestão da Diretriz de Segurança Corporativa

12.1. A diretriz D-PSC-001 é aprovada pelo Comitê Segurança da Informação

12.2. A presente diretriz foi aprovada no dia 11/10/2023

Eginaldo Oliveira Silva
DIRETOR DE OPERAÇÕES