Titulo:

Política de Segurança da Informação

Elaborado/Alterado por:

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - GTI

Aprovado por:

Diretoria Colegiada

1. OBJETIVO

Estabelecer diretrizes, visando a preservação dos recursos de Tecnologia da Informação da COMPESA, quanto à integridade, confidencialidade, autenticidade, disponibilidade da informação, redução dos riscos de erro humano e prevenção contra o uso indevido dos recursos de Tecnologia da Informação e Comunicação – TIC. A Política de Segurança da Informação tem por objetivo possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política auxilia manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

2. APLICAÇÃO

Este instrumento normativo se aplica a todas as áreas da Companhia Pernambucana de Saneamento, no que se refere ao uso dos recursos de Tecnologia da Informação.

3. DEFINIÇÕES

3.1. Acesso Remoto – Pode ser definido como a possibilidade de uma pessoa fora das dependências da Companhia se conectar e utilizar os recursos de sua rede.

3.2. Ameaça – Risco de um incidente indesejado que pode resultar em dano para um sistema ou para a organização.

3.3. Aplicação – Programa de computador (também conhecido pelo termo em inglês *software*) que auxilia o usuário a desempenhar uma atividade específica.

3.4. Ativo – Qualquer coisa, material ou imaterial, que tenha valor para a organização.

3.5. Autenticidade – Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

3.6. Computação em nuvem – Refere-se as funcionalidades de Tecnologia da Informação (sistemas, armazenamento, processamento, entre outros) entregues como serviço (pagos ou não) através de uma rede pública, comumente a Internet.

3.7. Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade.

3.8. Consentimento – Manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.

3.9. Dado(s) Pessoal(ais) – Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

3.10. Dado(s) Pessoal(ais) Sensível(eis) – Todo Dado Pessoal que pode gerar qualquer tipo de discriminação como, por exemplo, os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

3.11. Dado pessoal de criança e adolescente – Dado relativo a pessoas menores de 18 anos.

3.12. Disponibilidade – Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

3.13. Dispositivos Móveis – São equipamentos que permitem que os colaboradores executem suas atividades sem que seja necessário estar fisicamente em seu local de trabalho.

3.14. Gerência de Tecnologia da Informação e Comunicação (GTI) – Unidade organizacional responsável pela Infraestrutura de TI da COMPESA.

3.15. Incidente – Um incidente de Segurança da Informação pode ser definido como qualquer evento não esperado, confirmado ou sob suspeita, e que seja relacionado à segurança de sistemas de computação, redes de computadores, equipamentos da empresa ou que viole a Política ou os Guias de Segurança da Informação da Compesa.

3.16. Integridade – Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

3.17. LGPD – Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

3.18. Política de Segurança da Informação (PSI) – Diretrizes corporativas globais da Compesa sobre Segurança da Informação, conforme normativo GTI-POL-001/Compesa, que podem ser alteradas periodicamente.

3.19. Redes Sociais – Redes sociais são serviços de Internet onde pessoas ou organizações conectam-se para estabelecer algum tipo de relação online, que compartilham valores e objetivos comuns.

3.20. Segurança Cibernética – Ramo da segurança da informação que protege contra a ataques cibernéticos.

3.21. Segurança da Informação – ações que visam viabilizar e assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

3.22. Tratamento de incidentes – Trata-se do serviço que consiste em receber, filtrar, classificar e responder solicitações e alertas e realizar a identificação de tendências, bem como as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa.

3.23. Usuário (Colaborador) – Todo e qualquer empregado, terceiro ou estagiário que preste serviço para a Companhia.

4. RESPONSABILIDADES

4.1 Elaboração e alteração

A área gestora, a qual é responsável pela elaboração do presente normativo, a partir da identificação da necessidade de revisão e alteração do normativo, irá iniciar o processo de atualização, considerando mudanças nos procedimentos organizacionais, surgimento de novas atividades, melhorias nos processos, demandas das áreas relacionadas ao normativo e outras oportunidades de melhoria.

4.2 Revisão e aprovação

Após a elaboração, o normativo deverá ser submetido à revisão de conteúdo e padronização da Gerência de Excelência Organizacional (GEO) com posterior aprovação da Diretoria Colegiada na Reunião de Diretoria (REDIR), com formalização por meio de Resolução de Diretoria (RD).

4.3 Distribuição

A GEO será responsável por disponibilizar este normativo e suas alterações para todas as gerências/áreas interessadas e envolvidas no processo, utilizando o Sistema de Gestão de Normativos (SGN). A área gestora é responsável pela atualização do instrumento normativo quando disponibilizado fora do SGN.

4.4 Acesso

A visualização com cópia controlada do instrumento normativo será acessível a todas as gerências/áreas a que se aplica através do SGN e ao público externo por meio do site da COMPESA, quando aplicável.

4.5 Uso

A utilização do instrumento normativo será feita por todas as gerências/áreas envolvidas no processo.

4.6 Armazenamento e disponibilização

O armazenamento do instrumento normativo será virtual, sendo disponibilizado no SGN, com acesso pela intranet da Companhia. A área gestora é responsável pela publicação externa por meio do site da COMPESA, quando aplicável.

4.7 Preservação e recuperação

A preservação deste normativo será de responsabilidade da GGR. As solicitações de outras áreas para a consulta de versões anteriores do documento deverão ser feitas e aprovadas eletronicamente pelo SGN, sendo analisadas pela área gestora. A preservação e recuperação do normativo disponibilizada fora do SGN é de responsabilidade da área gestora.

4.8 Controle de alterações

O controle de alterações será feito pela área gestora e registrado no próprio documento, no campo “Histórico de alterações”, conforme item 8 deste normativo.

4.9 Retenção e disposição

Apenas a versão vigente do normativo estará acessível no SGN, estando as versões anteriores disponíveis para consulta apenas para a GGR e para a área gestora, bem como retidas em backups.

5. DETALHAMENTO

5.1 PREMISSAS

5.1.1 Proteger a informação corporativa, os segredos comerciais e industriais, visando a minimizar danos ao negócio, prevenir fraudes e maximizar o retorno dos investimentos e oportunidades de negócio, de acordo com sua sensibilidade e exposição ao risco.

5.1.2 Proteger as informações da Compesa ou sob a sua guarda quanto à confidencialidade, a integridade, a disponibilidade e a autenticidade.

5.1.3 Garantir condições para que os empregados sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de segurança adotados pela empresa.

5.1.4 Assegurar a adequação e a evolução das soluções de segurança para atender aos requisitos legais e contratuais, bem como impulsionar a inovação em soluções digitais entregando qualidade e segurança aos clientes.

5.1.5 Proteger os dados pessoais, a privacidade e o acesso à informação, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD) e ao normativo vigente da Compesa que trata da Política de Privacidade e Proteção de Dados Pessoais.

5.2 DETERMINAÇÕES

5.2.1 Sobre o Uso dos Ativos:

5.2.1.1 As informações, os serviços, os sistemas de informação e os recursos da Compesa e sob sua guarda devem ser protegidos contra ameaças, de forma a reduzir os riscos e a garantir as respectivas confidencialidade, integridade, disponibilidade e autenticidade, em alinhamento com os requisitos do negócio.

5.2.2 Sobre a Classificação da Informação:

5.2.2.1 Os ativos de informação classificados devem ser protegidos de uma forma consistente com o seu valor, requerimento legal, sensibilidade e criticidade para o negócio.

5.2.2.2 Todos os ativos de informação pertencentes à Compesa devem ser classificados a fim de garantir que estes recebam um nível adequado de proteção contra divulgação não autorizada, uso, modificação ou destruição, devendo sempre possuir um responsável pela sua geração, controle de acesso, guarda e classificação.

5.2.3 Sobre o Tratamento de Dados Corporativos, Dados Sensíveis e Dados Pessoais:

5.2.3.1 O uso de informações e recursos da Compesa deve se dar em consonância com as normas e padrões da Empresa, não devendo atender a necessidades particulares ou a qualquer finalidade estranha aos serviços.

5.2.3.2 O tratamento de dados pessoais deve seguir o normativo vigente da Compesa que trata da Política de Privacidade e Proteção de Dados Pessoais.

5.2.3.3 O tratamento dos dados pessoais de crianças e adolescentes deve se dar no melhor interesse de seus titulares. Os dados de crianças (menores de 12 anos) normalmente são tratados com o consentimento de, ao menos, um de seus responsáveis legais, com exceção das situações legais em que o consentimento não é exigido, como, por exemplo, na execução de serviço público.

5.2.3.4 A informação sobre o tratamento de dados pessoais sensíveis ou referentes a crianças ou adolescentes estará disponível em linguagem clara e simples, com concisão, transparência, inteligibilidade e acessibilidade, na forma da lei e de acordo com as regras do regime de tramitação sob segredo de Justiça.

5.2.4 Sobre o controle, monitoramento e gestão da Segurança Cibernética e da Informação:

5.2.4.1 A organização da segurança da informação deve ser estabelecida e mantida em ciclos de melhoria, por meio de ações coordenadas de governança e gestão, visando promover ambiente seguro e alinhado ao negócio.

5.2.4.2 A adoção de controles de segurança deve estar em conformidade com a legislação e normas vigentes, atender às necessidades dos serviços e suportar a evolução tecnológica, considerando os resultados da gestão de riscos e da gestão de vulnerabilidades técnicas.

5.2.4.3 O monitoramento da segurança deve ser realizado de forma permanente para identificar situações adversas visando a adoção de ações para minimizar impactos, inclusive nos casos em que tais situações envolvam violação de dado pessoal.

5.2.4.4 Os desvios e as falhas de segurança identificados não devem ser explorados ou utilizados indevidamente e devem ser reportados às áreas responsáveis. As violações de segurança devem ser registradas e as evidências caso encontradas devem ser protegidas de forma adequada, visando a subsidiar o tratamento de incidentes, a análise forense computacional e as necessidades de informação determinadas pela Lei.

5.2.4.5 A GTI será responsável pelo tratamento dos incidentes de segurança da informação.

5.2.4.6 A cultura de segurança da informação deve ser permanentemente fortalecida com a observância do trinômio “educação”, “treinamento” e “conscientização”, de forma a capacitar as pessoas nas suas atividades e a promover sua sensibilização para os temas.

5.2.5 Utilização de Dispositivos Móveis:

5.2.5.1 É responsabilidade do colaborador prezar pela proteção e segurança de dispositivos móveis, bem como das informações neles contidas.

5.2.5.2 Em caso de furto, roubo ou perda do equipamento, o colaborador deve informar imediatamente a ocorrência ao GTI. Posteriormente, deve providenciar um Boletim de Ocorrências (B.O.) policial e enviar o B.O. a GTI.

5.2.5.3 A GTI é responsável pela gestão dos dispositivos móveis na COMPESA, que consiste em atividades de monitoramento e controle. Todo dispositivo móvel está sujeito ao monitoramento da COMPESA.

5.2.5.4 São responsabilidades do proprietário, a guarda e manutenção adequada do dispositivo. A Compesa não se responsabiliza por acessos indevidos ao dispositivo ou danos de hardware e/ou software que possam ocorrer neste quando usado no contexto da instituição. A responsabilidade de proteção física e lógica do dispositivo é exclusiva do proprietário.

5.2.5.5 É responsabilidade exclusiva do proprietário do dispositivo a segurança dos dados no mesmo para não haver o vazamento de informações ou perda de dados.

5.2.6 Utilização das Contas de Correio:

5.2.6.1 O correio eletrônico deverá ser utilizado de forma consciente, responsável e para o melhor interesse da COMPESA, respeitando os princípios éticos na transmissão de mensagens.

5.2.6.2 A Compesa reserva-se o direito, sem qualquer notificação ou aviso, de monitorar, inspecionar, interceptar, ler, bloquear, retransmitir, redirecionar, copiar e divulgar para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, todas as mensagens enviadas por usuários através do seu sistema de correio eletrônico. Usuários ficam cientes e concordam com este monitoramento, não devendo possuir nenhuma expectativa de privacidade no uso desta ferramenta.

5.2.6.3 A Compesa reserva-se o direito de, em casos nos quais a segurança dos recursos do correio eletrônico seja ameaçada, eliminar e-mails e arquivos, bloquear conteúdos e usuários, permanente ou temporariamente.

5.2.7 Sobre a Identidade, Controle de Acesso e Acesso Remoto:

5.2.7.1 Os princípios relacionados com os privilégios mínimos, com a necessidade de conhecer e com a segregação de funções devem ser adotados nos processos de trabalho, de forma a reduzir o risco de modificação não-autorizada ou não intencional, ou o uso indevido dos ativos da Compesa.

5.2.7.2 Todo usuário deve ser representado digitalmente através de um identificador digital único, composto por conta de usuário e senha de acesso.

5.2.7.3 Todo acesso à informação ou ativo da Compesa, ainda que remoto, deve ser feito por meio da identidade digital individual e intransferível do usuário, sendo obrigatória a manutenção do caráter de exclusividade que esta possui.

5.2.7.4 É proibido, sob qualquer hipótese, o compartilhamento da identidade digital para qualquer finalidade.

5.2.7.5 O acesso remoto somente poderá ser utilizado por usuários autorizados pela GTI.

5.2.8 Sobre o Armazenamento de Arquivos e Cópias de Segurança:

5.2.8.1 As soluções de continuidade de negócios e de recuperação de desastres devem considerar controles que mantenham a segurança da informação a segurança cibernética e a proteção à privacidade nos níveis contratados.

5.2.8.2 Todos os arquivos armazenados nos dispositivos pertencentes à Compesa estão sujeitos à auditoria, coordenados pela Equipe de Segurança da Informação.

5.2.9 Sobre o Serviços de Terceirizados:

5.2.9.1 O acesso às informações, locais físicos, sistemas aplicativos e à rede de computadores, localmente ou através de acesso remoto, somente será permitido a terceirizados por meio de solicitação formal, aprovada pela GTI, pelo gestor responsável pelo contrato do terceirizado e pelo Responsável da Informação (caso o solicitante precise acessar informação sujeita a regras específicas de governança).

5.2.9.2 Deverá constar em todos os contratos da COMPESA informações acerca de “Acordo de Confidencialidade ou Cláusula de Confidencialidade”, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela Companhia.

5.2.9.3 Os funcionários terceirizados devem sempre estar portando o crachá de identificação de suas empresas em local visível.

5.2.9.4 O acesso aos locais, recursos, ativos e serviços da Compesa para os funcionários terceirizados necessário à execução das atividades profissionais deverá ser solicitado pelo gestor do contrato e devidamente autorizado pela GTI.

5.2.10 Sobre o Uso de Recursos da Intranet e da Internet:

5.2.10.1 Somente usuários autorizados deverão possuir acesso à Internet e Intranet da Compesa.

5.2.10.2 O acesso ao recurso corporativo de Internet oferecido pela Compesa deve ocorrer somente por meio de recursos ou dispositivos devidamente autorizados e/ou disponibilizados pela Compesa.

5.2.10.3 O acesso às redes sociais na Compesa é permitido apenas através de uma autorização específica e revogável ao usuário pela GTI.

5.2.10.4 O uso de aplicações na nuvem, externas ao ambiente da Compesa, estão limitadas a usuários autorizados pela GTI, e devem se restringir às aplicações homologadas pela Gerência de Tecnologia da Informação e Comunicação da COMPESA.

5.2.11 Sobre a Segurança Física:

5.2.11.1 As instalações, equipamentos, materiais e documentos da Compesa ou sob sua guarda devem estar protegidos contra ameaças.

5.2.11.2 A segurança física está diretamente ligada à classificação das informações armazenadas nas dependências da Compesa.

5.3 DISPOSIÇÕES FINAIS

5.3.1 A contração de serviços deve considerar os critérios de segurança da informação, de segurança cibernética, privacidade e proteção de dados definidas nesta Política.

5.3.2 A Política deve ser de conhecimento dos empregados, dos terceirizados e das empresas prestadoras de serviço.

5.3.3 A Política deve ser revisada a cada 2 (dois) anos ou nas situações que representem alterações significativas nos processos ou estrutura da Compesa.

5.3.4 A não observância da Política e seus desdobramentos normativos implicará a aplicação das sanções previstas nas normas disciplinares da Compesa.

6. INSTRUMENTOS NORMATIVOS RELACIONADOS

- GGR-POL-009 - Política de Privacidade e Proteção de Dados Pessoais

7. REFERÊNCIAS

1. LEI Nº 13.709. Lei Geral de Proteção de Dados (LGPD). D.O.U de 15/08/2018, pág. nº 59, 14 ago. 2018.
2. PORTARIA Nº 93. Portaria nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação. D.O.U. de 26/09/2019, pág. n 3, 2019.
3. ABNT NBR ISO/IEC 27002. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação., 2013.
4. ABNT NBR ISO/IEC 27001. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação., 2013.

8. HISTÓRICO DE ALTERAÇÕES

Nº da Versão	Data	Natureza da Revisão e/ou Alteração	RD vinculada
1	29/01/2021	Elaboração da versão Inicial do documento	RD 030/2020
2	29/01/2021	Versão atualizada e revisada.	SEI 0060500115.000897/2024-51

ANEXOS

ANEXO 1 - Guia de Proteção contra códigos maliciosos
Este documento define as regras para mecanismos e orientações para a proteção das informações da COMPESA contra códigos maliciosos.

ANEXO 2 - Guia de Gestão de incidentes de segurança
Este documento define as regras para o tratamento de incidentes de segurança da informação na COMPESA.

ANEXO 3 - Guia de Uso de dispositivos móveis
Este documento define as regras para o uso de dispositivos móveis na COMPESA.

ANEXO 4 - Guia de Contas de correio eletrônico
Este documento define regras e recomendações para o uso do Correio Eletrônico na COMPESA.

ANEXO 5 - Guia de Acesso remoto
Definir regras para o acesso remoto à rede corporativa e sistemas de informação da COMPESA.

ANEXO 6 - Guia de Classificação das informações
Este documento define as regras de como as informações da COMPESA devem ser classificadas com o objetivo de estabelecer os níveis de proteção adequados destas.

ANEXO 7 - Guia de Cópias de Segurança
Definir as regras para a execução de cópias de segurança das informações na COMPESA.

ANEXO 8 - Guia de Gestão de identidade e controle de acessos
Este documento define as regras para a criação de senhas e controle de acessos aos sistemas de informação da COMPESA.

ANEXO 9 - Guia de Armazenamento de arquivos
Este documento define as regras de responsabilidades, medidas de segurança, monitoramento e controle para o armazenamento de arquivos, e estabelece recomendações de bom uso para que não haja desperdício de recursos de armazenamento na COMPESA.

ANEXO 10 - Guia de Uso de redes sociais
Este documento define as regras para uso das redes sociais na Companhia Pernambucana de Saneamento.

ANEXO 11 - Guia de Gerenciamento de serviços de terceirizados
Este documento define as regras para o acesso de terceirizados a informações e ativos de TI da COMPESA.

ANEXO 12 - Guia de Uso de Internet e Intranet
Definir as regras de utilização da Internet e a Intranet na COMPESA.

ANEXO 13 - Guia de Gestão de ativos
Definir as regras e orientações para o uso e a proteção dos ativos da COMPESA.

ANEXO 14 - Guia de Uso de software
Definir as regras para aquisição, instalação e manutenção de software na COMPESA.

ANEXO 15 - Guia de Uso de informações na nuvem
Definir as regras para utilização de ferramentas de computação em nuvem na COMPESA.

ANEXO 16 - Guia de Segurança Física
Definir as regras de segurança física para todos os recursos que armazenam informações da COMPESA.

ANEXO 17 - Termo de Responsabilidade
Termo de Responsabilidade da Política de Segurança da Informação

ANEXO 18 - SEI 0060500115.000897/2024-51
N° SEI 0060500115.000897/2024-51