compesa

POLÍTICA

GTI-POL-001-01

Vigência: 29/01/2023

Titulo:

Política de Segurança da Informação

Elaborado/Alterado por:

GER DE TECNOLOGIA DA INFORMACAO E COMUNICACAO - 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 possibilita 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

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

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

c. Data Center – ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros.

d. Aplicação – Programa de computador que auxilia o usuário a desempenhar uma atividade específica (ex.: AutoCAD, para a área de engenharia e arquitetura; Skype, para telefonemas e conferências).

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

f. Autenticação – Processo que verifica se o usuário identificado é realmente quem ele diz ser, através do uso de sua senha pessoal ou de outros mecanismos (ex.: tokens e smartcards).

g. BYOD (Bring Your Own Device) – Traduzido literalmente como “traga seu próprio dispositivo móvel”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.

h. Login – Processo que permite a identificação, autenticação e autorização de acesso a um determinado sistema por um usuário. Também pode ser chamado de logon.

i. Software – Um termo genérico para definir um programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Essa sequência deve seguir padrões específicos que resultam em um comportamento desejado.

j. VPN (Rede Privada Virtual) – Conexão estabelecida sobre uma infraestrutura pública (internet), usando protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas.

k. Internet – é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos com o propósito de servir progressivamente usuários no mundo inteiro. É uma rede de várias outras redes, que consiste de milhões de empresas privadas, públicas, acadêmicas e de governo, com alcance local e global e que está ligada por uma ampla variedade de tecnologias de rede eletrônica, sem fio e ópticas.

l. Intranet – é uma rede de computadores privada que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local, como, por exemplo, a rede de uma empresa, que só pode ser acessada pelos seus utilizadores ou colaboradores internos.

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

A informação é um ativo de significativo valor para a COMPESA e que deve ser adequadamente protegido, desta forma, a adoção de políticas e guias que visem garantir a segurança da informação devem ser prioridades constantes da Companhia, reduzindo-se os riscos de danos, falhas e/ou os prejuízos que possam comprometer a imagem e os objetivos da Companhia.

A informação pode existir de diversas formas, pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou através de meio eletrônico, demostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que sempre seja protegida adequadamente.

Uma política (e o conjunto de guias associados) define diretrizes para o tratamento da informação criada, armazenada, processada ou transmitida no ambiente convencional ou de tecnologia da COMPESA, considerando dois objetivos fundamentais:

a. Orientar os funcionários, estagiários, fornecedores e terceiros da COMPESA a seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Companhia e do indivíduo.

b. Preservar as informações da COMPESA quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- Autenticidade: garantia ao receptor da correta identidade do emissor informado.
- Não-repúdio: garantia de que uma ação ou transação realizada não seja negada posteriormente por um emissor com autenticidade confirmada.
- Legalidade: garantia de que a informação está em conformidade com os requisitos legais e contratuais da organização e com o compromisso com os usuários e fornecedores.
- Auditabilidade: garantia de que a informação possa ser auditada.

5.1. Disposições Gerais

As informações e os sistemas de informação da COMPESA são ativos importantes e vitais aos negócios e devem ser protegidos de acordo com sua sensibilidade, valor e criticidade. Toda informação com as características abaixo não deve ser considerada de uso pessoal e não deve haver expectativa de privacidade sobre elas, independentemente de sua origem. São elas:

a) produzida ou recebida pelos funcionários da COMPESA no desempenho de suas funções profissionais;
b) produzida ou recebida pelos fornecedores e terceiros contratados como resultado da atividade profissional contratada pela COMPESA;
c) armazenada nos computadores, celulares, sistemas, servidores ou correio eletrônico da Companhia.

Está disponível no site http://intranet.compesa.com.br/wp-content/uploads/2016/08/Termo-de-Responsabilidade.pdf (Anexo XVII), o termo de responsabilidade que dá ciência ao colaborador a respeito das políticas e guias que devem ser cumpridos.

A Política de Segurança da Informação – PSI contém 16 guias que estão nos anexos desta política e publicadas no site http://intranet.compesa.com.br/infraestrutura/politica-de-seguranca/ e estão definidas conforme tabela abaixo:

Tabela 1 – Guias

#	Guia	Conteúdo
1	Proteção contra códigos maliciosos	Possui orientações para a proteção das informações da COMPESA contra códigos maliciosos (ex.: vírus)
2	Gestão de incidentes de segurança	Estabelece regras para o tratamento de incidentes de segurança, suspeita de quebra de segurança, assuntos pertinentes aos recursos de Internet/ Intranet ou furto, roubo ou perda de equipamentos, os quais deverão ser reportados imediatamente para serem investigados

#	Guia	Conteúdo
3	Uso de dispositivos móveis	Fornece orientação em relação ao uso de equipamentos móveis, tais como *notebooks*, *palmtops*, *laptops*, *tablets* e celulares corporativos
4	Contas de correio eletrônico	Apresenta regras para o uso do Correio Eletrônico
5	Acesso remoto	Estabelece regras para o acesso remoto (acesso a rede corporativa de computadores por meio da utilização da internet) aos sistemas de informação da COMPESA
6	Classificação das informações	Determina como as informações da COMPESA devem ser classificadas de acordo com o seu uso (ex.: confidencial, restrita, uso interno ou público) com o objetivo de estabelecer os níveis de proteção adequados para as mesmas
7	Cópias de Segurança	Define regras para a realização de cópias de segurança das informações da Companhia
8	Gestão de identidade e controle de acessos	Define regras para a criação de senhas e controle de acessos aos sistemas de informação da COMPESA
9	Armazenamento de arquivos	Define as responsabilidades, medidas de segurança, monitoramento e controle para o armazenamento de arquivos
10	Uso de redes sociais	Apresenta regras e condições para o uso das mídias sociais (ex.: Facebook, LinkedIn, etc.)
11	Gerenciamento de serviços de terceirizados	Descreve as regras e condições para que os terceirizados possuam acesso às informações e ativos de TI da COMPESA.
12	Uso de Internet e Intranet	Define regras para uso da Internet e a da Intranet.
13	Gestão de ativos	Apresenta regras que visam assegurar que os ativos de informação sejam adequadamente protegidos. Ativo é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos da COMPESA, como: base de dados, arquivos, diretórios de rede, etc.
14	Uso de software	Apresenta regras para aquisição, instalação e manutenção de software.
15	Uso de informações na nuvem	Apresentam as regras para utilização de ferramentas de computação em nuvem. Ferramentas de computação em nuvem são ambientes compartilhados (soluções na Internet a exemplo do Google Docs, SkyDrive, Dropbox, etc.) disponíveis para vários usuários, que visam o armazenamento de informações.
16	Segurança Física	Apresentam regras de segurança física para todos os recursos que armazenam informações da COMPESA.

A aplicação do que dispõe a presente Política será gerida pela GTI, que deverá orientar as áreas da COMPESA, visando a aplicação dos termos definidos nesta política.

- Eventual descumprimento identificado deverá ser comunicado à Diretoria respectiva, para adoção das providências cabíveis;
- Não será aceita como justificativa por eventual descumprimento do que nesta está determinado, para efeito de aplicação de penalidades previstas em guia específico, o desconhecimento do teor desta;
- Os casos omissos, relativos aos aspectos operacionais estabelecidos nesta Política, deverão ser resolvidos pela GTI.

Será de responsabilidade da Coordenação de Gestão de Pessoas (CGP) dar conhecimento da Política de Segurança da Informação e solicitar a assinatura no processo de admissão do termo de responsabilidade, Anexo 17 dessa Política.

5.2. Penalizações

O não cumprimento desta Política de Segurança da Informação e suas respectivos guias acarretará violação às regras internas da COMPESA e sujeitará o funcionário, fornecedor ou prestador de serviços às medidas administrativas e legais cabíveis, a serem julgadas pela Equipe de Segurança da Informação em conjunto com o Comitê Gestor de Segurança.

5.2.1. Penalidades para funcionários

Caso seja necessário advertir o funcionário ou tomar medidas administrativas, a Coordenação de Gestão de Pessoas (CGP) deve ser consultada acerca dos procedimentos para aplicar as seguintes formas de advertências:

- Advertência por escrito: Será encaminhado ao funcionário um comunicado informando o descumprimento da política, com a indicação precisa da violação praticada. Uma cópia desse comunicado permanecerá arquivada na respectiva pasta do funcionário;
- Suspensão: A pena de suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade;
- Demissão por justa causa: nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho (CLT);
- Demais medidas administrativas previstas nos regulamentos internos da Companhia.

5.2.2. Penalidades para o prestador de serviços

O prestador de serviços poderá ser penalizado através do cancelamento de seu contrato e/ou aplicação de multas contratuais conforme criticidade da infração cometida, além das punições legais cabíveis como consequência de atos ilícitos praticados.

5.3. Abrangência da Política

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Os padrões e requisitos contemplados nesta Política devem ser aplicados de forma mandatória para todos os ativos da Companhia, sempre com o apoio da Alta Administração (Presidente e Diretores), aos quais cabem disponibilizar os recursos necessários para a sua viabilização, bem como assegurar seu cumprimento.

5.4. Regrais Gerais

O **Anexo 6 - Guia de classificação das informações** determina como as informações da COMPESA devem ser classificadas com o objetivo de estabelecer os níveis de proteção adequados para as mesmas. As informações poderão ser examinadas ou monitoradas a qualquer momento sem notificação ao usuário. A assinatura do **Anexo 17 - Termo de responsabilidade da Política de Segurança das Informações,** implica na concordância do usuário das informações com os termos aqui descritos.

As informações referentes aos negócios da COMPESA devem circular em meios seguros fornecidos pela Companhia. Os funcionários da Companhia não estão autorizados a produzir ou manter informações em equipamentos pessoais ou em serviços disponíveis ao público em geral não homologados para uso na Companhia pela GTI.

Todas as solicitações de inclusão ou manutenção de acesso de contas de usuários aos sistemas de informação deverão ser registradas na ferramenta de *Service Desk*, disponível na intranet, e aprovadas pelo Gestor da área responsável pela informação, conforme detalhado no **Anexo 8 - Guia de Gestão de identidade e controle de acessos**.

Somente serão permitidos acessos remotos às informações da Companhia, através da utilização de equipamentos corporativos ou homologados que utilizarem os controles de segurança homologados pela área de TI. Vide detalhes no **Anexo 5 - Guia de Acesso Remoto**.

O acesso de funcionários terceirizados às informações, locais, sistemas aplicativos e à rede de computadores somente será permitido por meio de solicitação e aprovação formal. Deverá constar em todos os contratos da COMPESA o Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que o acesso às informações possa ser concedido. Vide detalhes no **Anexo 11 - Guia de Gerenciamento de serviços de terceirizados**.

Todos os computadores da Companhia ou que necessitem estar conectados à rede corporativa deverão possuir software antivírus e *antimalware* homologado pelo setor de TI da COMPESA. Vide detalhes no **Anexo 1 - Guia de Proteção contra códigos maliciosos**.

Não é permitida a utilização de equipamentos de informática (exceto celulares) de propriedade particular nas dependências da COMPESA, assim como não é permitida a conexão dos mesmos e de celulares particulares à rede corporativa (ou a qualquer recurso corporativo). Vide detalhes no **Anexo 3 - Guia de Uso de dispositivos móveis.**

Não é permitido o uso de correios eletrônicos particulares (Hotmail, Gmail, Yahoo, UOL, etc.) nos equipamentos da Companhia, conforme descrito no guia de Uso de Correio Eletrônico. As regras de uso de correio eletrônico estão descritas no **Anexo 4 – Guia de Uso de correio eletrônico.**

Somente é permitido o uso de “modems 3G” em equipamentos corporativos para acesso à Internet em situações de deslocamento, onde o colaborador não tenha acesso à rede corporativa segura. Vide detalhes no **Anexo 12 - Guia de Uso de Internet e Intranet.**

Somente é permitida a realização de cópias (“download”) de arquivos na Internet para fins profissionais, ou seja, relacionados aos negócios da COMPESA, e desde que esteja conforme todos os guias vigentes. Vide detalhes no **Anexo 12 - Guia de Uso de Internet e Intranet.**

O acesso às redes sociais será permitido apenas para funcionários cujas atribuições funcionais requeiram estes acessos, e mediante autorização específica pelo Comitê de Gestão da Segurança da Informação. Vide detalhes no **Anexo 10 - Guia de Uso de redes sociais.**

Não é permitida a transferência ou o armazenamento de informações da COMPESA em ferramentas disponíveis para o público em geral, que utilizem computação em nuvem, como, por exemplo, Dropbox, Sendspace, Google Docs, Skydrive, Prezi, Slideshare, Rapidshare, entre outros. Vide detalhes no **Anexo 15 - Guia de Uso de informações na “nuvem”**. Não é permitido o armazenamento de informações no ambiente computacional da COMPESA que contenham conteúdo ou assuntos particulares. Vide detalhes no **Anexo 9 - Guia de Armazenamento de arquivos.**

Somente softwares homologados, instalados e adquiridos legalmente pelo setor de Tecnologia da Informação devem ser utilizados nos computadores pertencentes a COMPESA. Vide detalhes no **Anexo 14 - Guia de Uso de software**.

Todos os ativos fixos de TI (Ex.: notebooks, desktops, aparelhos celulares, etc.) devem ser examinados antes de serem descartados, para assegurar que os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança. Vide detalhes no **Anexo 13 – Guia de Gestão de ativos**.

Incidentes de segurança da informação deverão ser comunicadas à GTI, preferencialmente através da ferramenta de *Service Desk*, conforme detalhado no **Anexo 2 – Guia de Gestão de Incidentes de Segurança**.

5.5. Responsabilidades

A responsabilidade pela segurança da informação é de todos os colaboradores da COMPESA e varia de acordo com as funções e atribuições destes. São elas:

5.5.1. Colaboradores (funcionários, estagiários e prestadores de serviços)

- Cumprir fielmente e fazer cumprir a Política de Segurança da Informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;
- Comunicar imediatamente à Equipe de Segurança da Informação qualquer incidente de segurança detectado.

5.5.2. Alta Administração (Presidente e Diretores)

- Aprovar a Política de Segurança da Informação e suas revisões;
- Apoiar, dar o exemplo e exigir o comprometimento de todos os colaboradores e terceiros da Companhia para com esta Política de Segurança da Informação.

5.5.3. Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação será criado com a finalidade de estabelecer políticas e diretrizes para segurança da informação.

- Analisar criticamente a aplicação da Política de Segurança da Informação;
- Aprovar a Política de Segurança da Informação;
- Propor mudanças, ajustes ou melhorias da Política de Segurança da Informação;
- Definir o plano estratégico para implantação da Política de Segurança da Informação;
- Definir e aprovar junto às diretorias da COMPESA, os procedimentos e penalidades para fazer cumprir a Política de Segurança da Informação;
- Validar os casos de exceções à Política de Segurança da Informação;

- Mobilizar os gestores para o cumprimento da Política de Segurança da Informação;
- Acompanhar a execução da Política de Segurança da Informação;
- Analisar os riscos e impactos aos ambientes e aos negócios provenientes de mudanças emergenciais;
- Deliberar sobre as violações da Política de Segurança da Informação, definindo as penalidades que serão aplicadas.

5.5.4. Equipe de Segurança da Informação

Equipe responsável por garantir que a Política de Segurança da Informação seja implantada e cumprida conforme os guias estabelecidaos neste documento. Será composta por membros da GTI, que atuam na área de segurança do ambiente computacional da COMPESA.

- Atualizar a política e guias de Segurança da Informação sempre que houver alteração no ambiente computacional, atualizações tecnológicas, ou mudanças organizacionais que o justifiquem, a fim de manter e melhorar o nível de segurança, encaminhando as novas versões para aprovação do Comitê Gestor de Segurança da Informação;
- Apoiar a TI da COMPESA na definição de soluções técnicas para adequação de seus ambientes computacionais a esta Política de Segurança da Informação, quando solicitado;
- Implantar a Política de Segurança da Informação;
- Prover ampla divulgação da Política de Segurança da Informação para todos os colaboradores da COMPESA;
- Oferecer orientação e treinamento sobre a Política de Segurança da Informação, seus guias e instruções específicas a todos os colaboradores da COMPESA;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Monitorar o cumprimento da Política de Segurança da Informação, encaminhando aos respectivos gestores as ocorrências de descumprimento dos guias de Segurança por seus subordinados, para as providências cabíveis;
- Avaliar o nível de segurança alcançado, emitindo relatórios periódicos de Análise de Riscos à Diretoria e ao Comitê Gestor de Segurança;
- Tomar as providências de emergência, conforme plano e ação de resposta a incidentes sob responsabilidade da Equipe de Segurança da Informação, imediatamente após detecção ou conhecimento de incidentes de segurança no âmbito do ambiente computacional da COMPESA;
- Definir e aplicar as medidas e contramedidas necessárias para correção de problemas causados por quebra ou fragilidade da Política de Segurança da Informação, encaminhando ao respectivo gestor da área envolvida relatório técnico sobre o ocorrido e as respectivas providências tomadas, bem como as recomendações de segurança a serem seguidas;
- Mobilizar os gestores para o cumprimento da Política de Segurança da Informação;
- Desenvolver e implantar processos e procedimentos operacionais necessários para a execução, controle e avaliação da Política de Segurança da Informação;
- Assegurar a disponibilização atualizada, de todos os documentos relacionados a esta Política de Segurança da Informação.

5.5.5. Departamento Jurídico (Gerência de Contencioso e Consultivo – GCC)

- Auxiliar a Equipe de Segurança da Informação e o Comitê Gestor de Segurança no que diz respeito aos aspectos legais;
- Assegurar a capacitação do time jurídico para o tratamento de temas relacionados à Segurança da Informação;
- Orientar o Comitê Gestor de Segurança da Informação quanto às providências jurídicas aplicáveis para casos de incidentes de segurança envolvendo colaboradores ou terceirizados;
- Avaliar, quando solicitado pelo Comitê Gestor da Segurança da Informação, os guias de Segurança da Informação.

5.5.6. Responsável pela Informação

Os “responsáveis pela informação” são indivíduos que lideram departamentos na Companhia, e são responsáveis pela segurança das informações que controlam (por exemplo: o gestor de RH é o responsável pelas informações cadastrais dos funcionários), isto é, informações que estão de sua responsabilidade direta. No papel de responsável por algum tipo de informação, o colaborador deve:

- Definir a classificação das informações sob sua responsabilidade, com base nos critérios de classificação constantes no Anexo 6 - Classificação das Informações;
- Cumprir e fazer cumprir a Política de Segurança da Informação;

- Assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação;
- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da Companhia às autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, considerando a matriz de cargos e funções, a Política e as Guias de Segurança da Informação da Companhia;
- Manter registro e controle atualizado de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando/solicitando o cancelamento para aquelas que não forem necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela GTI, com o objetivo de identificar desvios em relação à Política e às Guias de Segurança da Informação, tomando as ações corretivas necessárias;
- Comunicar imediatamente à Equipe de Segurança da Informação eventuais casos de violação de segurança da informação e participar da investigação dos incidentes;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão da Segurança da Informação, prestando os esclarecimentos solicitados.

5.5.7. Departamento de Recursos Humanos

- Incorporar em seus processos práticas que assegurem a divulgação e cumprimento desta política e guias associados;
- Colher a assinatura do Termo de Responsabilidade dos funcionários, terceirizados e estagiários, arquivando-o nas respectivas pastas funcionais;
- Informar prontamente à Equipe de Segurança da Informação todos os desligamentos, afastamentos e modificações no quadro funcional da COMPESA.

6. INSTRUMENTOS NORMATIVOS RELACIONADOS

7. REFERÊNCIAS

AGU – Política de Segurança da Informação e das Comunicações – Diretrizes e Normas. Disponível em: http://www.agu.gov.br/page/content/detail/id_conteudo/228893. Acesso em mar. 2018.

Diógenes, Yuri; Mauser, Danel - Certificação Security + da Prática Para o Exame SYO-301, Editora Nova Terra, São Paulo: 2011.

Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu de – Política de Segurança da Informação – Guia Prático para Elaboração e Implantação 2ª Edição Revisada, Editora Ciência Moderna, Rio de Janeiro: 2008.

Fontes, Edison – Políticas e Normas para a Segurança da Informação, Editora Brasport, Rio de Janeiro: 2012.

BRASIL. Decreto-Lei n. 5.452, de 1 de maio de 1943. Consolidação das Leis do Trabalho (CLT), Brasília, DF, maio 1943.

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

ANEXOS

ANEXO 1 - Proteção contra códigos maliciosos

Possui orientações para a proteção das informações da COMPESA contra códigos maliciosos (ex.: vírus)

ANEXO 2 - Gestão de incidentes de segurança
Estabelece regras para o tratamento de incidentes de segurança, suspeita de quebra de segurança, assuntos pertinentes aos recursos de Internet/ Intranet ou furto

ANEXO 3 - Uso de dispositivos móveis
Fornece orientação em relação ao uso de equipamentos móveis, tais como notebooks, palmtops, laptops, tablets e celulares corporativos

ANEXO 4 - Contas de correio eletrônico
Apresenta regras para o uso do Correio Eletrônico

ANEXO 5 - Acesso remoto
Estabelece regras para o acesso remoto (acesso a rede corporativa de computadores por meio da utilização da internet) aos sistemas de informação da COMPESA

ANEXO 6 - Classificação das informações
Determina como as informações da COMPESA devem ser classificadas de acordo com o seu uso

ANEXO 7 - Cópias de Segurança
Define regras para a realização de cópias de segurança das informações da Companhia

ANEXO 8 - Gestão de identidade e controle de acessos
Define regras para a criação de senhas e controle de acessos aos sistemas de informação da COMPESA

ANEXO 9 - Armazenamento de arquivos
Define as responsabilidades, medidas de segurança, monitoramento e controle para o armazenamento de arquivos

ANEXO 10 - Uso de redes sociais
Apresenta regras e condições para o uso das mídias sociais (ex.: Facebook, LinkedIn, etc.)

ANEXO 11 - Gerenciamento de serviços de terceirizados
Descreve as regras e condições para que os terceirizados possuam acesso às informações e ativos de TI da COMPESA

ANEXO 12 - Uso de Internet e Intranet
Define regras para uso da Internet e a da Intranet.

ANEXO 13 - Gestão de ativos
Apresenta regras que visam assegurar que os ativos de informação sejam adequadamente protegidos.

ANEXO 14 - Uso de software

Apresenta regras para aquisição, instalação e manutenção de software.

ANEXO 15 - Uso de informações na nuvem

Apresentam as regras para utilização de ferramentas de computação em nuvem.

ANEXO 16 - Segurança Física

Apresentam regras de segurança física para todos os recursos que armazenam informações da COMPESA.

ANEXO 17 - Termo de Responsabilidade

Termo de Responsabilidade