

CARTILHA

SEGURANÇA DA INFORMAÇÃO



SUMÁRIO

CONTEXTUALIZAÇÃO

1. SEGURANÇA DA INFORMAÇÃO

- 1.1. Definição
- 1.2. Termos associados
 - 1.2.1. Confidencialidade
 - 1.2.2. Disponibilidade
 - 1.2.3. Integridade
 - 1.2.4. Privacidade
 - 1.2.5. Controles

2. POTENCIAL DE INCIDENTES

- 2.1. Definição
- 2.2. Ameaças
- 2.3. Vulnerabilidades
- 2.4. Risco

3. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

- 3.1. Definição
- 3.2. Backup
- 3.3. Senhas
- 3.4. Sites suspeitos



4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- 4.1. Definição
- 4.2. Política de Backup e de Restauração
- 4.3. Plano de Contingencia
- 4.4. Normas de Segurança da Informação
- 4.5. Conclusão

5. REFERÊNCIAS

CONTEXTUALIZAÇÃO

O uso constante de dispositivos móveis e computadores expõe os usuários a riscos no mundo virtual. Para reduzir esses riscos, devemos promover uma cultura de segurança da informação. Esta cartilha fornece orientações para o uso seguro de recursos virtuais.

OBJETIVOS DA CARTILHA



- Conceituar o termo segurança da informação e suas implicações.
- Relacionar dados resultantes de ameaças encontradas no mundo virtual e boas práticas para redução de danos.
- Recomendar a Política de Segurança da Informação da Prefeitura Municipal de Salvador - PSI-PMS.

Dada a importância do tema e a existência da cartilha, viu-se que a contribuição será efetiva para o aumento/elevação do nível de conhecimento do(a) usuário(a) sobre a utilização dos recursos eletrônicos do **Fundo Municipal da Previdência de Salvador**.

SEGURANÇA DA INFORMAÇÃO

1.1 Definição

A segurança da informação visa **garantir a confidencialidade, disponibilidade e integridade dos dados, aplicando controles para minimizar os riscos de incidentes** (ISO 27.000, 2018; VAKHTER e colab, 2021). Os sistemas de Tecnologia da Informação - TI devem seguir as normas **ABNT NBR ISO/IEC 27.701** (gestão da privacidade) e **ABNT NBR ISO/IEC 29100:2020** (estrutura de privacidade em sistemas de TI). A segurança da informação é um dos princípios de privacidade da **ABNT NBR ISO/IEC 29100:2020**, que define valores para a proteção de dados pessoais em sistemas de Tecnologias da Informação e Comunicação - TIC. A conscientização em segurança da informação é um controle eficaz para mitigar vulnerabilidades, já que o usuário é o elo mais frágil (SASSE e colab., 2001).



SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

1.2.1. Confidencialidade

O conceito de confidencialidade de acordo com a ISO 27.000:2018, ***é a propriedade de um sistema que impede a disponibilização ou divulgação de informações a indivíduos, entidades ou processos não autorizados.***

Em essência, a confidencialidade garante que a informação seja acessível apenas a quem tem o direito de vê-la.

Imagine a caixa-forte onde você guarda seus segredos mais importantes. **Confidencialidade é exatamente isso:** a garantia de que as informações sensíveis ou privadas só serão acessadas por quem tem permissão para vê-las. É como manter um segredo guardado a sete chaves.

Acontece o tempo todo no nosso dia a dia:

- **Sua consulta médica:** Quando você conversa com seu médico, ele tem o dever de manter suas informações de saúde em sigilo. Ele não pode sair contando para todo mundo sobre o que você tem ou o seu tratamento. Isso é confidencialidade.
- **Seu extrato bancário:** As informações sobre quanto dinheiro você tem na conta, suas compras e pagamentos são confidenciais. Só você e o banco podem ver esses detalhes.

SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

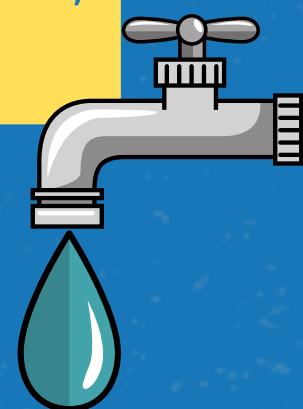
1.2.2. Disponibilidade

O conceito de confidencialidade de acordo com a ISO 27.000:2018, *é a propriedade de um sistema que impede a disponibilização ou divulgação de informações a indivíduos, entidades ou processos não autorizados.*

Imagine que você precisa de algo e quer ter certeza de que estará lá, funcionando e pronto para ser usado, sempre que você precisar. **Disponibilidade é exatamente isso:** a garantia de que um serviço, um produto ou uma informação estará acessível e operacional no momento em que você precisar.

Acontece o tempo todo no nosso dia a dia:

- **Água na torneira:** Quando você abre a torneira, espera que saia água, certo? Você espera que o serviço de água esteja "disponível" 24 horas por dia. Se não sair água, ele não está disponível.
- **Energia elétrica:** Ao acender a luz, você espera que ela ligue. Se houver um apagão, a energia não está disponível.
- **Seu telefone celular:** Você espera que ele esteja funcionando e com sinal quando você precisa fazer uma ligação ou usar a internet. Se ele trava ou fica sem sinal, não está disponível.



SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

1.2.3. Integridade

O conceito de integridade de acordo com a ISO:27000:2018, *é a propriedade de exatidão e completude. Essa característica de um sistema garante que a informação seja precisa e completa, evitando que o conteúdo seja alterado ou corrompido.*

Imagine que você tem um documento muito importante, como uma receita de bolo ou um contrato. Integridade é a garantia de que esse documento está completo, exato e não foi modificado, alterado ou danificado por ninguém não autorizado. É como ter certeza de que a informação é verdadeira e confiável.

Acontece o tempo todo no nosso dia a dia:

- **Um contrato assinado:** Depois que um contrato é assinado, espera-se que nenhuma cláusula seja alterada. Se alguém mudar algo depois da assinatura, a integridade do contrato foi quebrada, e ele perde sua validade e confiança.
- **Um termômetro:** Você confia que o termômetro está marcando a temperatura correta. Se ele estiver descalibrado ou quebrado e mostrar uma temperatura errada, a integridade de sua medição está comprometida.



SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

1.2.4. Privacidade

A Lei Geral de Proteção de Dados (LGPD), *Lei nº 13.709/2018*, regula o tratamento de dados pessoais em meios físicos e digitais (GOVERNO FEDERAL DO BRASIL, 2018). A ABNT NBR ISO/IEC 29100:2020 enfatiza a proteção da privacidade desses dados, especialmente os sensíveis. A ISO/IEC 27000:2018, que trata da segurança da informação, ressalta a importância de soluções técnicas para garantir a privacidade, em conformidade com a LGPD e a ABNT NBR ISO/IEC 29100:2020.

Privacidade é exatamente isso: é o seu direito de controlar quem tem acesso às suas informações pessoais, ao seu espaço, às suas escolhas e às suas interações, e como essas informações são usadas.

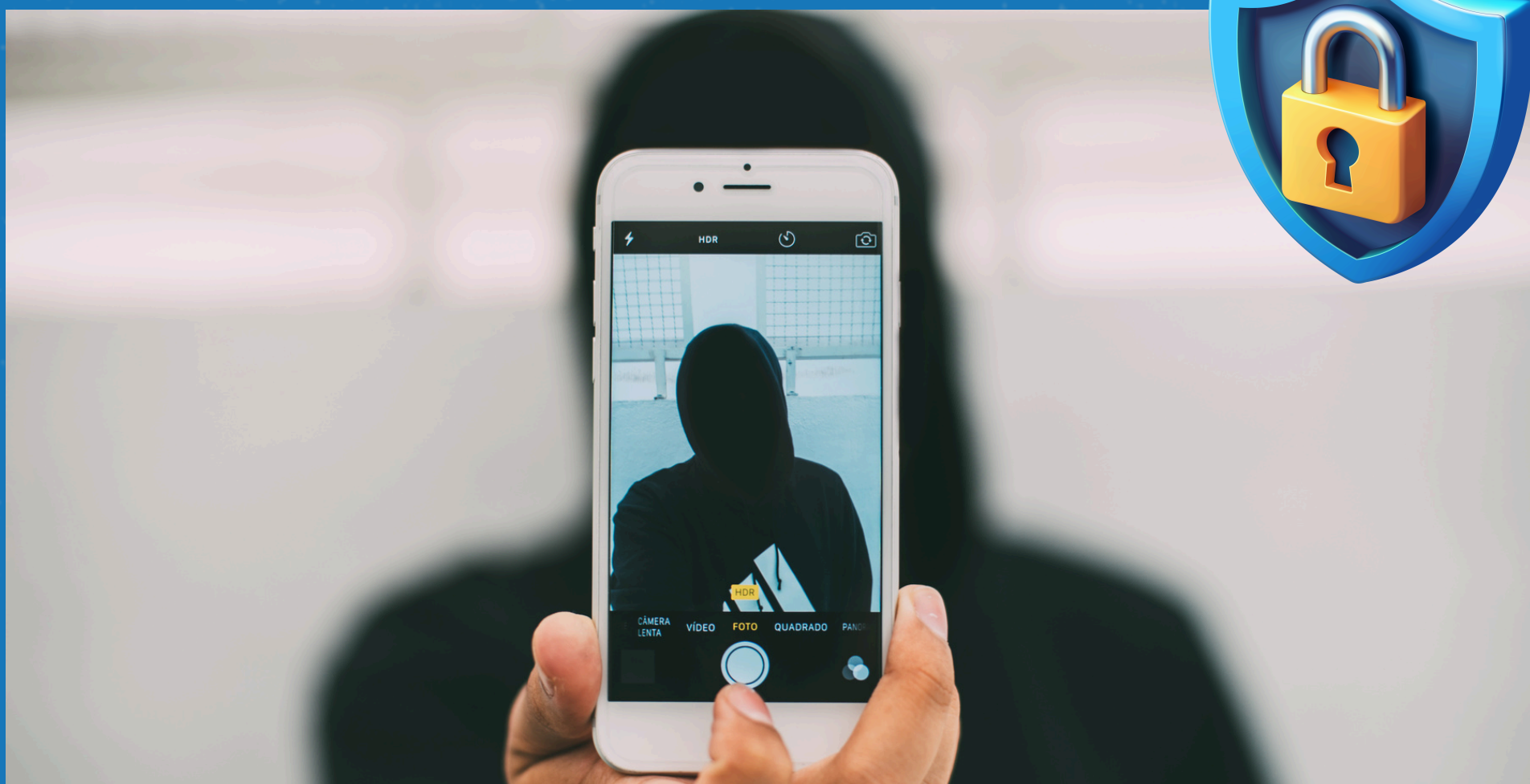


SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

Acontece o tempo todo no nosso dia a dia:

- **Sua casa:** Você decide quem entra na sua casa, quando entra e o que vê lá dentro. Fechar a cortina ou trancar a porta é exercer sua privacidade.
- **Uma conversa particular:** Quando você fala em voz baixa com alguém sobre um assunto pessoal, você está buscando privacidade para aquela conversa, esperando que ninguém mais ouça.



SEGURANÇA DA INFORMAÇÃO

1.2. Termos associados e suas implicações

1.2.5. Controles

De acordo com a ISO/IEC 27005:2019, *controles são medidas implementadas para tratar riscos, reduzindo sua probabilidade e/ou impacto. Cada atividade possui um risco inerente que, após os controles, torna-se risco residual. Esses controles devem ser adequados, proporcionais e eficazes no contexto da organização.*

Controle é o conjunto de regras, ações ou mecanismos que você coloca em prática para garantir que as coisas aconteçam do jeito certo, que os objetivos sejam alcançados e que nada indesejado aconteça. É como ter o leme de um barco, direcionando para onde ele deve ir.

Acontece o tempo todo no nosso dia a dia:

- **Sinal de trânsito:** O semáforo é um controle. Ele dita quando você pode ir e quando deve parar, para que o trânsito flua e acidentes sejam evitados.
- **As regras de um jogo:** Em um jogo, as regras controlam o que os jogadores podem ou não fazer, garantindo que o jogo seja justo e divertido para todos.
- **Câmeras de segurança:** Elas são um controle para monitorar e inibir ações indesejadas, protegendo um local.

POTENCIAL DE INCIDENTES

2.1. Definições

Em segurança da informação, ameaças, vulnerabilidades e riscos são conceitos interligados que descrevem o **potencial de incidentes de segurança e seus impactos**. Uma ameaça é qualquer evento ou causa potencial de um incidente indesejado, como um ataque cibernético. Uma vulnerabilidade é uma fraqueza que pode ser explorada por uma ameaça, como um sistema desatualizado. O risco é a probabilidade de uma ameaça explorar uma vulnerabilidade e causar um impacto negativo. Em resumo, a ameaça ataca a vulnerabilidade, e o risco é a chance de esse ataque acontecer e causar danos.

Compreender a relação entre **ameaças, vulnerabilidades e riscos** é fundamental para a **segurança da informação**. Ao identificar e analisar as ameaças e vulnerabilidades, é possível avaliar os riscos e implementar medidas de segurança adequadas para proteger as informações e sistemas.



POTENCIAL DE INCIDENTES

2.2. Ameaças

Segundo a ABNT NBR ISO/IEC 27005:2019, *ameaças são causas potenciais de incidentes indesejados que podem resultar em danos a um ativo ou organização*. Já a ISO/IEC 27001 destaca que a identificação de ameaças é essencial para o processo de análise de risco e para definir controles eficazes de segurança da informação.

Imagine que você tem algo que valoriza muito, como sua casa, seu dinheiro ou sua saúde. Uma ameaça é qualquer coisa que tem o potencial de causar um dano ou prejuízo a essa coisa valiosa. É um perigo em potencial.

Acontece o tempo todo no nosso dia a dia:

- **Comida estragada:** Se você come algo que venceu ou não foi bem conservado, a comida é uma ameaça à sua saúde.
- **Um ladrão:** Uma pessoa com intenção de roubar é uma ameaça ao seu patrimônio ou à sua segurança.
- **Um incêndio:** Para uma floresta, uma fagulha pode ser uma ameaça, pois pode iniciar um grande incêndio.
- **Um buraco na rua:** Para o seu carro, um buraco é uma ameaça, pois pode danificar os pneus ou a suspensão.



POTENCIAL DE INCIDENTES

2.3. Vulnerabilidades

Conforme a ABNT NBR ISO/IEC 27005:2019, *vulnerabilidade é uma fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças*. A ISO/IEC 27001 complementa ao indicar que identificar vulnerabilidades é essencial para avaliar riscos e implementar controles que garantam a proteção da informação.

Imagine que você tem algo que quer proteger, mas ele tem um ponto fraco, uma falha. Uma vulnerabilidade é exatamente esse ponto fraco, essa falha que, se for descoberta por alguém ou uma ameaça, pode causar um problema ou um dano.

Acontece o tempo todo no nosso dia a dia:

- **Uma casa com a janela destrancada:** A janela destrancada é a vulnerabilidade. Um ladrão (a ameaça) pode se aproveitar dessa falha para entrar na casa.
- **Uma ponte com uma rachadura na estrutura:** A rachadura é uma vulnerabilidade. O peso excessivo (ameaça) pode fazer com que a ponte ceda nesse ponto fraco.
- **Um carro com pneus gastos:** Os pneus gastos são uma vulnerabilidade. Uma pista molhada (a ameaça) pode fazer com que o carro derrape, porque os pneus não têm aderência suficiente.

POTENCIAL DE INCIDENTES

2.3. Vulnerabilidades

Conforme a ABNT NBR ISO/IEC 27005:2019, *vulnerabilidade é uma fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças*. A ISO/IEC 27001 complementa ao indicar que identificar vulnerabilidades é essencial para avaliar riscos e implementar controles que garantam a proteção da informação.

Imagine que você tem algo que quer proteger, mas ele tem um ponto fraco, uma falha. Uma vulnerabilidade é exatamente esse ponto fraco, essa falha que, se for descoberta por alguém ou uma ameaça, pode causar um problema ou um dano.



POTENCIAL DE INCIDENTES

2.4. Riscos

Acontece o tempo todo no nosso dia a dia:

- **Atravessar a rua sem olhar:** O risco é a chance de ser atropelado (a probabilidade) e quão grave seria se acontecesse (o impacto: um machucado ou algo grave).
- **Deixar o fogão ligado e sair de casa:** O risco é a chance de acontecer um incêndio (probabilidade) e o estrago que ele faria na sua casa (o impacto).
- **Não usar cinto de segurança no carro:** O risco é a chance de se machucar gravemente em um acidente (probabilidade de acidente + impacto do ferimento).



BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.1. Definições

São um conjunto de diretrizes, procedimentos e controles recomendados para proteger dados e sistemas contra ameaças, **garantindo confidencialidade, integridade e disponibilidade** da informação. Elas envolvem ações preventivas, detecção de incidentes, resposta a falhas, gestão de acessos, atualização de sistemas e conscientização de usuários, alinhadas a normas como a ISO/IEC 27001 e 27002.

Para essa cartilha, traremos as boas práticas que são informadas pela **Política de Segurança da Informação da Prefeitura Municipal de Salvador** (PSI da PMS).

A Política de Segurança da Informação da Prefeitura Municipal de Salvador (PMS) estabelece uma série de boas práticas e diretrizes para a correta utilização dos materiais e dados do município. A mesma se baseia em diversas leis e normas para garantir a segurança das informações e dos recursos de Tecnologia da Informação (TI), como exemplo das leis federais, Lei Federal nº 12.527 (Lei de Acesso à Informação - LAI), Lei Nº 9.609 (uso de software não licenciado), Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), ABNT NBR ISO/IEC 27002:2022, ABNT NBR ISO/IEC 27001:2022, ABNT NBR ISO/IEC 20000-1:2011, Normas NBR ISO/IEC 27701, 27018, 27005 e 29134, National Institute of Standards and Technology (NIST) CSF: SP 800-40.

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.2. Backup

Backup é o processo de criar cópias de dados em um local separado, a fim de proteger esses dados contra perda ou corrupção. O objetivo principal do backup é permitir a recuperação de informações em caso de falhas de hardware, exclusão acidental, ataques cibernéticos, desastres naturais ou outros eventos que possam comprometer os dados originais. Essencialmente, é uma cópia de segurança que garante a disponibilidade e a integridade das informações.

É como ter um "plano B" para suas informações digitais, garantindo que você não fique sem elas se algo der errado com o original.

Acontece o tempo todo no nosso dia a dia:

- **Se o seu celular quebrar ou for roubado:** Se você fez backup das suas fotos e contatos, você não os perdeu para sempre. Basta pegar um novo celular e "colar" suas informações de volta.
- **Se o seu computador der problema:** Arquivos importantes de trabalho ou estudo podem ser recuperados se você tiver uma cópia guardada.
- **Para evitar sustos:** É uma forma de se prevenir contra imprevistos, como um arquivo que você apaga sem querer

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.3. Senhas

Uma senha é uma sequência secreta de caracteres (letras, números, símbolos) usada para verificar a identidade de um usuário e conceder acesso a sistemas, contas online, dispositivos ou informações protegidas. Ela serve como uma chave digital para proteger a privacidade e a segurança dos dados.

Em resumo, a senha é sua primeira linha de defesa no mundo digital, e cuidar bem dela é essencial para proteger sua privacidade e suas informações.



BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.3. Senhas

No dia a dia, a senha é como a chave da sua casa digital. Assim como você usa uma chave para trancar a porta da sua casa e proteger seus pertences, a senha serve para:

- **Proteger suas contas:** É o que te permite entrar no seu e-mail, nas redes sociais, no banco online ou em qualquer aplicativo que guarda suas informações. Sem a senha, ninguém consegue acessar.
- **Manter seus segredos seguros:** Ela impede que pessoas não autorizadas vejam suas conversas, fotos pessoais ou informações financeiras.
- **Garantir que você é você:** Quando você digita sua senha, é como se estivesse apresentando sua identidade digital para o sistema, provando que é o dono daquela conta.



BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.4. Sites suspeitos

Sites suspeitos são páginas da internet que, intencionalmente ou não, representam um risco à segurança do usuário e de seus dados. Eles são frequentemente criados para enganar, infectar dispositivos com malware, roubar informações pessoais ou financeiras (phishing), ou disseminar conteúdo impróprio/ilegal. A "suspeita" surge de características incomuns ou alarmantes no design, no endereço (URL), nas solicitações de dados, ou nas promessas que fazem.

No dia a dia, um site suspeito é como uma "armadilha digital" que tenta te enganar.

Sinais para identificar um site suspeito:



- **Erros de português ou layout fora de padrão:** O site apresenta erros de escrita e imagens de baixa qualidade. Sites sérios geralmente têm um visual profissional.
- **Mensagens muito alarmantes ou ofertas incríveis:** "Sua conta foi bloqueada, clique aqui AGORA!" ou "Você ganhou um prêmio que nunca se inscreveu!". Essas são táticas para te fazer agir sem pensar.
- **Não tem o "cadeadinho":** Na barra de endereço do navegador, um cadeado fechado significa que a conexão é segura. Se não tem cadeado ou aparece "Não seguro",

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.1. Definição

A Política de Segurança da Informação (PSI) é um conjunto de diretrizes, regras e procedimentos que uma organização estabelece para proteger seus ativos de informação.

Para a ABNT ISO/IEC, a PSI é a declaração formal da organização sobre como a segurança da informação será gerenciada, servindo como base para todos os outros controles e processos de segurança.

Para a LGPD, a PSI serve como um documento fundamental que detalha as estratégias, procedimentos e responsabilidades para garantir a segurança, privacidade e conformidade no tratamento de dados pessoais.

A Política de Segurança da Informação da Prefeitura Municipal de Salvador foi instituída pelo Decreto N° 38.116 de 16 de janeiro de 2024.

PSI da PMS tem como objetivo principal:

- **Orientar todos os seus usuários para assegurar a efetividade da direção de gestão e suporte à segurança da informação.**
- **Garantir a conformidade com os requisitos legais, estatutários, regulatórios e contratuais na PMS.**



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.2. Política de Backup e de Restauração

A política de backup e restauração é abordada no "**Plano de Backup e Restauração de Arquivos Digitais**" dentro da Política de Segurança da Informação (PSI) da Prefeitura Municipal de Salvador (PMS). De forma resumida, ela estabelece as seguintes boas práticas:

- **Realização de backups regulares:** Os dados devem ser copiados periodicamente.
- **Definição de frequência e retenção:** É necessário determinar com que frequência os backups são feitos e por quanto tempo os dados copiados serão mantidos.
- **Transporte e armazenamento seguros:** As mídias de backup devem ser transportadas e armazenadas de forma segura para evitar perdas ou acessos não autorizados.
- **Testes regulares de restauração:** Os backups devem ser testados periodicamente para garantir que os dados possam ser restaurados com sucesso em caso de necessidade.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.4. Normas de Segurança da Informação

Diversas normas de segurança da informação são estabelecidas pela PSI da PMS, que são diretrizes e regras a serem seguidas para **proteger os dados e os recursos de TI do município**. Algumas das principais normas incluem:

- **Uso da Internet:** Define regras para o uso aceitável da internet e mídias sociais, incluindo a necessidade de usar os recursos para fins oficiais, controles de acesso, requisitos para conexões de rede seguras, e proibições de acesso a conteúdos impróprios ou ilegais.
- **Acesso a Recursos de TI:** Detalha a concessão e gestão de acessos aos sistemas, exigindo credenciais pessoais e intransferíveis, gerenciamento rigoroso de senhas, revisão periódica dos direitos de acesso e responsabilidades dos usuários.
- **Uso do Correio Eletrônico:** Regula o uso do e-mail corporativo, limitando-o a atividades profissionais, proibindo conteúdo inadequado, e estabelecendo diretrizes para anexos, remetentes e assinaturas.
- **Plano de Resposta a Incidentes de Segurança:** Descreve os passos para lidar com incidentes cibernéticos, desde a detecção até a recuperação, com foco na melhoria contínua dos processos.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.5. Conclusão

A Política de Segurança da Informação da Prefeitura Municipal de Salvador (PMS) estabelece um conjunto abrangente de boas práticas com o objetivo primordial de proteger as informações e os recursos de TI do município. Essas práticas visam criar um ambiente digital seguro e responsável para todos os usuários. Em resumo conclusivo, as boas práticas da PMS focam nos seguintes pilares:

1. Gestão da Informação: Classificação e manuseio seguro de dados.
2. Uso Seguro dos Recursos: Orientação para uso responsável de internet, e-mail e sistemas.
3. Controle de Acessos: Gestão rigorosa de permissões e senhas.
4. Resiliência a Riscos: Prevenção e resposta a ameaças, incluindo backups e planos de contingência.
5. Governança e Conformidade: Aderência a normas e leis para garantir responsabilidade e segurança contínuas.

Em suma, as boas práticas da PMS são construídas sobre os pilares da governança, proteção, responsabilidade e resiliência, visando salvaguardar o patrimônio informacional do município e garantir a continuidade dos serviços públicos.

REFERÊNCIAS

- DECRETO Nº 38.116 de 16 de janeiro de 2024: Política de Segurança da Informação da Prefeitura Municipal de Salvador.
- Lei Geral de Proteção de Dados Pessoais, ou Lei nº 13.709/2018.
- ABNT NBR ISO/IEC 27.000.
- ABNT NBR ISO/IEC 27.002.
- ABNT NBR ISO/IEC 27.701.
- ABNT NBR ISO/IEC 29.100.

